Search RISKS using swish-e

THE RISKS DIGEST

Forum on Risks to the Public in Computers and Related Systems

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

Index to Volume 4

Saturday, 6 June 1987

THE RISKS DIGEST

Forum On Risks To The Public In Computers And Related Systems

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

Search RISKS using swish-e

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

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

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

Feeds

RSS 1.0 (full text)

RSS 2.0 (full text)

ATOM (full text)

RDF feed

WAP (latest issue)

Simplified (latest issue)

Smartphone (latest issue)
Under Development!!

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

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

Selectors for locating a particular issue from a volume

Volume number: Volume Issue Number: Issue

Get Specific Issue

Volume Index

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

Index to the RISKS Digest

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

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

Search RISKS using swish-e

THE RISKS DIGEST

Forum on Risks to the Public in Computers and Related Systems

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

Volume 4: Issue 1

Sunday, 2 November 1986

Contents

ILLUSTRATIVE RISKS TO THE PUBLIC IN THE USE
OF COMPUTER SYSTEMS AND RELATED TECHNOLOGY
Compiled by Peter G. Neumann (1 November 1986),
Chmn ACM Committee on Computers and Public Policy

A compendium of all of the following cases is in preparation, anthologizing back issues of ACM SIGSOFT Software Engineering Notes [SEN], references to which are cited below as (SEN vol no); e.g., (SEN 11 5) is October 1986, one vol per year, quarterly (plus an occasional special issue). Some incidents are well documented, others need further study. Please send corrections, additions, and refs to PGNeumann, SRI International, BN168, Menlo Park CA 94025, phone 415-859-2375, ARPANET Neumann@CSL.SRI.COM or RISKS@CSL.SRI.COM.

Legend: ! = Loss of Life; * = Potentially Life-Critical; $ = Loss of Resources
S = Security/Privacy/Integrity Problem; ["\" = multiply listed item]
H = Human directly implicated (e.g., user/administrator/operator/penetrator)
[NOTE: Design, implementation flaws are human problems, but not marked "H".]

SPACE:
!!$$ Shuttle Challenger explosion, 7 killed. [Booster sensors (removed) might have permitted early detection of booster leak?] [28 Jan 86] (SEN 11 2)
$ First Space Shuttle backup launch-computer synch problem (SEN 6 5: Jack Garman, "The bug heard 'round the world", October 1981, pp. 3-10.)
* Second Shuttle simulation: bug found in jettisoning an SRB (SEN 8 3)
* Second Space Shuttle operational simulation: tight loop upon cancellation of an attempted abort; required manual override (SEN 7 1)
$ Titan 34D, Nike Orion, Delta-178 failures follow Challenger (SEN 11 3)
* Columbia return delayed; computer malfunctioned despite redundancy (SEN 9 1)

* Columbia near-disaster, liquid oxygen drained mistakenly just before launch, computer output misread (SEN 11 5)
*$ Delays of two Discovery shuttle launches due to backup computer outage [second one on 25 Aug 85] [NY Times 26 August 1985] (SEN 10 5)
* Discovery laser aims upside down: +10,023 miles instead of feet (SEN 10 3)
* Shuttle Discovery landing gear -- correlated faults (SEN 10 3)
* Shuttle STS-6 bugs in live Dual Mission software precluded aborts (SEN 11 1)
* Mercury astronauts forced into manual reentry? (SEN 8 3)
*$ Mariner 1: Atlas booster launch failure DO 3 I=1.3 (not 1,3)? (SEN 8 5,11 5)
*$ Mariner 18: aborted due to missing NOT in program (SEN 5 2)
* Gemini V 100mi landing err, prog ignored orbital motion around sun (SEN 9 1)
$ Atlas-Agena software missing hyphen; $18.5M rocket destroyed (SEN 10 5)
$ Aries with $1.5M payload lost: wrong resistor in guidance system; (SEN 11 5)
* TDRS relay satellite locked on wrong target (SEN 10 3)
* Cosmic rays halve shuttle Challenger comm for 14 hours [8 Oct 84] (SEN 10 1)
$ Viking had a misaligned antenna due to a faulty code patch (SEN 9 5)
* Ozone hole over South Pole observed, but denied by SW for 8 years (SEN 11 5)

MISSILE, AIR, AND NAVAL DEFENSE:
!!$ Sheffield sunk during Falklands war, 20 killed. Call to London jammed antimissile defenses. Exocet on same frequency. [AP 16 May 86](SEN 11 3)
** Returning space junk detected as missiles. Daniel Ford, The Button, p. 85
** WWMCCS false alarms triggered scrams [3-6 Jun 1980] (SEN 5 3, Ford pp 78-84)
** DSP East satellite sensors overloaded by Siberian gas-field fire (Ford p 62)
(Ford summarized in SEN 10 3)
** BMEWS at Thule detected rising moon as incoming missiles [5 Oct 1960] (SEN 8 3). See E.C. Berkeley, The Computer Revolution, pp. 175-177, 1962.
** SAC/NORAD: 50 false alerts in 1979 (SEN 5 3), incl. a simulated attack whose outputs accidentally triggered a live scramble [9 Nov 1979] (SEN 5 3);
*$ Libyan bomb raid accidental damage by "smart bomb" (SEN 11 3)
* Frigate George Philip fired missile in opposite direction (SEN 8 5)
* Unarmed Soviet missile crashed in Finland. Wrong flight path? (SEN 10 2)
* Tomahawk cruise missile failure: program erased [8 Dec 86] (SEN 11 2)
* 2nd Tomahawk failure (SEN 11 5). Bit dropped by HW triggered ABORT sequence.
* Sgt York (DIVAD) radar/anti-aircraft gun -- software problems (SEN 11 5)
$ Software flaw in sub-launched ballistic missile system (SEN 10 5)
$ AEGIS failures on 6 of 17 targets attributed to software (SEN 11 5)
- WWMCCS computers' comm reboot failed by blocked multiple logins (SEN 11 5)
$ Armored Combat Earthmover 18,000 testing missed serious problems (SEN 11 5)
$ Stinger missile too heavy to carry, noxious to user (SEN 11 5)
$ "Spy ship" Liberty: 3 independent warnings to withdraw all lost (SEN 11 5)
** Strategic Defense Initiative -- debate over feasibility (SEN 10 5)

MILITARY AVIATION:
!!$ Handley Page Victor tailplane broke, crew lost. 3 INDEPENDENT test methods. 3 independent flaws, masking flutter problem (SEN 11 2,p.12;correct'n 11 3)
*$ F-18 crash due to missing exception cond. Pilot OK (SEN 6 2, more SEN 11 2)
* F-18 missile thrust while clamped, plane lost 20,000 feet (SEN 8 5)
* F-16 simulation: plane flipped over whenever it crossed equator (SEN 5 2)
* F-16 simulation: upside-down, deadlock over left vs. right roll (SEN 9 5)
$H F-16 landing gear raised while plane on runway; bomb problems (SEN 11 5)
*$ F-14 off aircraft carrier into North Sea; due to software? (SEN 8 3)
*$ F-14 lost to uncontrollable spin, traced to tactical software (SEN 9 5)
$S Pres.Reagan's command plane jams thousands of garage-door openers (SEN 11 2)

COMMERCIAL AVIATION:
!!$H Korean Airlines 007 shot down killing 269 [1 Sept 1983]; autopilot left on
HDG 246 rather than INERTIAL NAV? (NYReview 25 Apr 85, SEN 9 1, SEN 10 3)
!!$H Air New Zealand crashed into Mt Erebus, killing 257 [28 Nov 1979];
computer course data error detected but pilots not informed (SEN 6 3 & 6 5)
!!H Aeromexico flight to LAX crashes with private plane, 82 killed (SEN 11 5)
!!$ DC-10 indicators failed: their power came from missing engine (SEN 11 5)
!!$ Electra failures due to simulation omission (SEN 11 5)
!$ Computer readout for navigation wrong, pilot killed (SEN 11 2)
*H South Pacific Airlines, 200 aboard, 500 mi off course near USSR [6 Oct 1984]
*H 747SP (China Air) autopilot tried to maintain 41,000 ft after engine failed,
other engines died in stall, plane lost 32,000 feet [19 Feb 85] (SEN 10 2)
* Avionics failed, design used digitized copier-distorted curves (SEN 10 5)
** 767 (UA 310 to Denver) four minutes without engines [August 1983] (SEN 8 5)
* 767 failure LA to NY forced to alternate SF instead of back to LA (SEN 9 2)
* Air Traffic Control data cable loss caused close calls (SEN 10 5)
* FAA Air Traffic Control: many computer system outages (e.g., SEN 5 3, 11 5),
near-misses not reported (SEN 10 3)

RAIL TRAVEL:
!!$H Canadian trains collide despite "safe" computer; 26 killed (SEN 11 2)
* SF BART train doors opened between stations during SF-Oakland leg (SEN 8 5)
- SF BART automatic control disastrous days of computer outages (SEN 6 1)
- SF Muni Metro: Ghost Train reappeared, forcing manual operation (SEN 8 3)

AUTOMOBILES:
!$ Mercedes 500SE with graceful-stop no-skid brake computer left 368-foot
skid marks; passenger killed (SEN 10 3)
*S Sudden auto acceleration due to interference from CB transmitter (SEN 11 1);
*$ Microprocessors in 1.4M Fords, 100K Audis, 350K Nissans, 400K Alliances/
Encores, 140K Cressidas under investigation (SEN 10 3)
*$ El Dorado brake computer bug caused recall of that model [1979] (SEN 4 4)
*$ Ford Mark VII wiring fires: flaw in computerized air suspension (SEN 10 3)

MOTOR VEHICLE DATABASE PROBLEMS:
!!H Bus crash kills 21, injures 19; computer database showed driver's license
had been revoked, but not checked? Also, unreported citation (SEN 11 3)
*SH British auto citations removed from database for illicit fee (SEN 11 1)
$ California DMV computer bug hid $400 million fees for six months (SEN 11 2)
$ Toronto motor vehicle computer reported $36 million extra revenue (SEN 11 3)
- Alaskan DMV program bug jails driver [Computerworld 15 Apr 85] (SEN 10 3)

ELECTRICAL POWER (NUCLEAR AND OTHER):
!!$H Chernobyl nuclear plant fire/explosion/radiation [26 April 86] (SEN 11 3)
Misplanned experiment on emergency-shutdown recovery procedures backfired.
Fatal (at least 31), serious cases continue to mount. Wide-spread effects.
*$ 14 failures in Davis-Besse nuclear plant emergency shutdown (SEN 11 3)
*$ Three Mile Island PA, now recognized as very close to meltdown (SEN 4 2),
with 4 equipment failures plus misjudgement. SW flaw noted (SEN 11 3)
!!,$ Various previous nuclear accidents -- American (3 deaths SL-1 Idaho Falls)
Soviet (27-30 deaths on Icebreaker Lenin, three other accidents) (SEN 11 3)
* Subsequent to Chernobyl, US Nuclear Regulatory Commission relaxed fire

isolation guidelines, enabling a fire to wipe out two systems (SEN 11 3)
*$ Crystal River FL reactor (Feb 1980) (Science 207 3/28/80 1445-48, SEN 10 3)
*$ Great Northeast power blackout due to threshold set-too-low being exceeded
*$ Power blackout of 10 Western states, propagated error [2 Oct 1984](SEN 9 5)
* Ottawa power utility loses working three units to faulty monitor (SEN 11 5)
* Reactor overheating, low-oil indicator; two-fault coincidence (SEN 8 5)
* Bug discovered in Shock II model/program for designing nuclear reactors to withstand earthquakes shuts down five nuclear power plants (SEN 4 2)

MEDICAL HEALTH AND SAFETY RISKS:
!,* Misprogrammed cancer radiation machines; 1 killed, 2 injured (SEN 11 3)
! Woman killed daughter, tried to kill son and self; "computer error" blamed for false report of their all having an incurable disease (SEN 10 3)
! Arthritis-therapy microwaves set pacemaker to 214, killed patient (SEN 5 1)
! Retail-store anti-theft device reset pacemaker, man died (SEN 10 2, 11 1)
* Pacemaker locked up when being adjusted by doctor (SEN 11 1)
* Failed heart-shocking devices due to faulty battery packs (SEN 10 3)
* Multipatient monitoring system recalled; mixed up patients (SEN 11 1)
* Diagnostic lab instrument misprogrammed (SEN 11 1)
* AI medical system in Nevada gave wrong diagnosis, overdose (SEN 11 2)
* Video display terminal health safety a continuing concern (SEN 11 3, 11 5)
* Dangers of computerized robot used in surgery (SEN 10 5)

ROBOTS AND ARTIFICIAL INTELLIGENCE:
! Japanese mechanic killed by malfunctioning Kawasaki robot (SEN 10 1, 10 3) [Electronic Engineering Times, 21 December 1981]
! At least 4 more, possibly 19 more robot-related deaths in Japan (SEN 11 1)
! Michigan man killed by robotic die-casting machinery (SEN 10 2, 11 1)
! Chinese computer builder electrocuted by his smart computer. (WWN headline: "Jealous Computer Zaps its Creator" after he built newer one...) (SEN 10 1)
* Two cases of robot near-disasters narrowly averted by operators (SEN 11 3)
- Servant robot runs amok, winds up in court (SEN 11 5)

OTHER CONTROL-SYSTEM PROBLEMS:
!!$,H? 1983 Colorado River flood, faulty data/model? Too much water held back prior to spring thaws; 6 deaths, $ millions damage [NY Times 4 Jul 1983]
*$ Union Carbide leak (135 injuries) exacerbated by program not handling aldicarb oxime plus operator error [NY Times 14 and 24 Aug 85] (SEN 10 5)
*$ Computer-controlled turntable for huge set ground "Grind" to halt (SEN 10 2)
*$ 8080 control system dropped bits and boulders from 80 ft conveyor (SEN 10 2)
- Titanic photo expedition control program erratic (SEN 11 5)

OTHER COMPUTER-AIDED DESIGN PROBLEMS:
* Hartford Civic Center Roof collapse due to use of wrong model (SEN 11 5)
* Salt Lake City shopping mall roof collapses on first snowfall (SEN 11 5)
* John Hancock Building in Boston glass panels kept falling out (???)

FINANCIAL LOSSES:
$ $32 BILLION overdraft at Bank of New York (prog counter overflow) (SEN 11 1)
$H $2 Billion goof due to test tape being rerun live (SEN 11 2)
$H .5M transaction became $500M, due to "000" convention; $200M lost (SEN 10 3)
$ Slow responses in Bankwire interface SW resulted in double posting of tens of $millions, with interest losses (SEN 10 5)
$ California state computer wrote $4M checks accidentally (SEN 11 5)

$H ATM accepts lollipop cardboard as $1M (New Zealand) deposit (SEN 11 5)
$H ATM money dispensers blocked and emptied later by youths (SEN 11 5)
$H Barclays Bank hacked for 440,000 pounds? (SEN 11 5)
$H ATMs gave $140,000 on VISA card over a weekend -- software glitch (SEN 11 2)
$ Program bug permitted auto-teller overdrafts in Washington State (SEN 10 3)
$ IRS reprogramming delays; interest paid on over 1,150,000 refunds (SEN 10 3)
$H San Jose library lost two weeks of records. Books, fines lost. (SEN 11 3)
$H Video quiz game scam -- teams of "experts" with right answers (SEN 11 5)

STOCK-MARKET PHENOMENA:
$ Computer-induced big stock-market swings (SEN 11 2, 11 5)
$ Vancouver Stock Index lost 574 points over 22 months -- roundoff (SEN 9 1)
$ NY Stock Exch. halted for 41 minutes; drum channel errors killed primary
and backup computer systems [24 Feb 72]
$ London Stock Exchange computer system crashes [23 May 86]
$ Hurricane Gloria in NY closes Midwest Stock Exchange (SEN 11 1)

TELEPHONE PROBLEMS:
$ Pac Bell loses $51 million on lost phone-call charges (SEN 11 3)
$ 400 pay phones in Hackensack lost charges for half of the calls (SEN 11 3)
$ GTE Sprint incomplete SW changes lost $10-$20M in Feb/Mar/Apr 86 (SEN 11 3)
$ GTE Sprint billing errors from botched daylight savings cutover (SEN 11 5)
*$ Michigan Bell ESS office, 2 long outages. SW updates in progress. (SEN 11 3)
*$ 707 area code (above San Fran.) shut down completely for 5 hours (SEN 11 5)
$* Atlanta telephone system down for 2 hours (SEN 11 5)
*$ C&P computer crashes 44,000 DC phones (SEN 11 1)
$ C&P computer "tape flaws" delay 100,000 bills by two months (SEN 11 5)
$ 1979 AT&T program bug downed phone service to Greece for months (SEN 10 3)
$ Ghost phone calls to 911 from cordless phone interference (SEN 11 2)
$H Swedish phone bill of $2600 -- program error plus human error (SEN 11 5)

ELECTION PROBLEMS:
SH Election frauds, lawsuits (SEN 11 3, 11 5), mid-stream patches in HW/SW (SEN
10 3, 10 4), David Burnham, NY Times, 7/29, 7/30, 8/4, 8/21, 12/18 1985.
- Clerical error blamed for election computer program mishap (SEN 11 5)
- Quebec election prediction bug: wrong pick [1981] (SEN 10 2 pp 25-26, 11 2)

INSURANCE FRAUDS:
$SH Possible fraud on reinsurance -- message time stamp faked??? (SEN 10 5)
$H N-step reinsurance cycle; software checked for N=1 and 2 only (SEN 10 5)

COMPUTER SECURITY/PRIVACY/INTEGRITY VIOLATIONS: PENETRATIONS,
BLACKMAIL, TROJAN HORSES AND VIRUSES, TIME-BOMBS, PRANKS,
SPOOFS, SCAMS, AND OTHER PROBLEMS
..... General comments:
*SH Many known security flaws in computer operating systems and application
programs. Discovery of new flaws running way ahead of their elimination.
Flaws include problems with passwords, superuser facilities, networking,
reprogrammable workstations, inadequate or spoofable audit trails, ease
of perpetrating viruses and Trojan horses, improper handling of line
breaks, etc. Examples of UNIX flaws as illustrative. Lots of internal
fraud, but external penetrations frequent.
..... Penetrations by nonauthorized personnel:

SH "Captain Midnight" preempted Home Box Office program (SEN 11 3, 11 5)
SH Chernenko at MOSKVAX: network mail hoax [1 April 1984] (SEN 9 4)
SH 1984 Rose Bowl hoax, scoreboard takeover ("Cal Tech vs. MIT") (SEN 9 2)
$SH TRW Credit information bureau breakins -- one involved gaining information
on Richard Sandza (Newsweek reporter who wrote ``anti-hacker'' articles)
and running up $1100 in charges. (SEN 10 1)
SH British Telecom's Prestel Information Service -- demonstration for
a reporter read Prince Philip's demo mailbox and altered a financial market
database [London Daily Mail 2 Nov 84] (SEN 10 1)
Break-in being prosecuted (1st such prosecution in Britain) (SEN 11 3)
SH Milwaukee 414s broke into many computers (some with guessable passwords)
*SH Santa Clara prison data system (inmate altered release date) (SEN 10 1).
$SH Reps Zschau, McCain computers penetrated, mailings affected (SEN 11 2)
SH Grade-changing prank at Stanford (around 1960) (SEN 8 5)
$SH Southwestern Bell computer penetrated: free long-distance calls (SEN 11 3)
$SH Bloodstock Research thoroughbred horse-genealogy computer system penetrated
$SH Debit card copying easy despite encryption (DC Metro, SF BART, etc.)
$SH Microwave phone calls interceptable; cordless, cellular phones spoofable
$SH Callback security schemes rather easy to break (SEN 11 5 from RISKS-3.29)
SH Systematic breakins of Stanford UNIX systems via network software (SEN 11 5)
Brian Reid, "Lessons from the UNIX Breakins at Stanford", pp 29-35, Oct 1986
..... Trojan Horses
$SH PC Graphics program Trojan horse (ArfArf) wiped out users' files (SEN 10 5)
SH Another Trojan horse trashes DOS -- NOTROJ (SEN 11 5)
$SH Harrah's $1.7 Million payoff scam -- Trojan horse chip (SEN 8 5)
SH C compiler Trojan horse for UNIX trapdoor (Ken Thompson, "Reflections on
Trusting Trust", 1983 Turing Award Lecture, CACM 27 8, August 1984)
..... Internal perpetrations:
$SH Nevada slot-machine ripe for $10 to 15 million phony payoffs? (SEN 11 2)
*SH San Fran. Public Defender's database readable by police; as many as 100
cases could have been compromised [Feb 1985] (SEN 10 2)
\SH Election frauds by vendor? by operations staff? (SEN 11 3),... [see above]
*SH British auto citations removed from database for illicit fee (SEN 11 1)
*SH Software time-bomb inserted by unhappy programmer (for extortion?) (10 3)
*SH Los Angeles Water&Power computer system software time-bomb (SEN 10 3)
SH DC analyst in dispute with boss changed password on city computer (SEN 11 2)
S Sabotage of Encyclopedia Brittania database (SEN 11 5)
$SH "Goodbye, folks" software prank costs perpetrator 1000 pounds (SEN 11 3)
*S Air Force sells off uncleared tapes with sensitive data (SEN 11 5)
$SH Embezzlements, e.g., Muhammed Ali swindle [$23.2 Million], Security Pacific
[$10.2 Million], City National Beverly Hills CA [$1.1 Million, 23 Mar 1979]
Marginally computer-related, but suggestive of things to come?

UNINTENTIONAL DENIALS OF SERVICE:
* ARPANET ground to a complete halt; accidentally-propagated status-message
virus [27 Oct 1980] (SEN 6 1: Reference -- Eric Rosen, "Vulnerabilities of
network control protocols", SEN, January 1981, pp. 6-8)
- Gobblings of legitimate automatic teller cards (SEN 9 2, 10 2, 10 3, 10 5)
- Royal Wedding side-effect shuts down computer machine room? (SEN 11 5)
* Central computer for Austin auto traffic lights & 2 lights out (SEN 11 5)
$ Computer crash stops gasoline pumps (SEN 11 5)
$ Many cases of point-of-sale systems crashing, business lost (SEN 11 5)
- Program bug in Computerized Coke machines caused many phone calls (SEN 10 2)
- Network node hit by lightning; down for weeks (SEN 11 5)

$H IRS has no contingency plans for computer disasters (GAO report) (SEN 11 2)
- VMS tape backup SW trashed disc directories dumped in image mode (SEN 8 5)
---> Denials of Service/Interference of Communications ('\' = noted above):
\!! Sheffield (20 deaths), pacemakers (2 deaths),
*$ Challenger communications, CB auto interference, Ghost phone calls,
\$ telephone outages, hurricane closes Midwest Stock Exchange,
\$ bug in "Grind" stage set software halts production,
\- Pres.Reagan's command plane; Sputnik effects on garage doors

AGGRAVATION TO INDIVIDUALS OR TO THE POPULACE AT LARGE:
$H Whistleblowing aerospace SW Quality Assurer fired, life threatened(SEN 11 3)
* Carrier control unit blamed for nuclear false alarm (SEN 11 5)
$S Sputnik frequencies triggered garage-door openers
$ Customer declared dead by bank computer; effects propagated (SEN 11 3)
$ Demo NatComm thank-you mailing mistitled supporters [NY Times, 16 Dec 1984]
- Earthquakes: 3 of 5 reported never happened; microwave static (SEN 11 5)
H Query of vacationing programmer starts beer panic (SEN 11 5)
H Indian program to reroute bus lines trounced (SEN 11 5)
- British school examination program gave erroneous grades (SEN 11 5)
*H Various cases of false arrest due to computer database use (SEN 10 3,11 1)
\- Various cases of gobbled bank cards

LEGAL IMPLICATIONS:
!$ Deaths of 3 lobstermen in storm not predicted by National Weather Service --
3 mos unrepaired weather buoy; $1.25M award (SEN 10 5) [NY Times 13 Aug 85]
Overturned by federal appeals court. [AP, 15 May 86] (SEN 11 3)
** Launch on warning legality subject of law suit (SEN 10 2, 11 5)
$ Sex-therapy software risks (SEN 11 2)
$ Computerized sex ring broken; records seized (SEN 11 5)
$ Israeli supreme court appeal blamed on computer malfunction (SEN 11 5)
*$ Expert systems for criminal investigations (SEN 11 5)
$H Lawsuit against Symphony for leaving out proposal section (SEN 11 5)
S Concern over privacy of Swedish Databank (SEN 11 5)

MISCELLANEOUS COMPUTER HARDWARE/SOFTWARE PROBLEMS:
- Clock setting algorithm gets wrong time; other clock problems (SEN 11 2)
$ Tape unit caught on fire from repeated reading of tape section (SEN 5 1)
- Some destructive computer puns
H Incidents on people's willingness to trust computers (SEN 11 5)
- See also anecdotes from ACM Symposium on Operating Systems Principles,
SOSP 7 (SEN 5 1) and follow-on (SEN 7 1).

Search RISKS using swish-e

Report problems with the web pages to the maintainer

Search RISKS using swish-e

THE RISKS DIGEST

Forum on Risks to the Public in Computers and Related Systems

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

Volume 4: Issue 2

Sunday, 2 November 1986

Contents

Insurgent Squirrel Joins No-Ways Arc [Title adapted by PGN from

Ross McKenrick <CRMCK%BROWNVM.BITNET@WISCVM.WISC.EDU>
Thu, 30 Oct 86 11:40:40 EST

1957 Bob Ashenhurst hoax
on Rick Gould's PhD Thesis]

"Lost Squirrel Causes Troublesome Power Surge"
Providence Journal, Thursday, October 30, 1986

An electrical power surge caused computers to go on the blink in Providence brokerage houses, banks, and office buildings yesterday. A Narragansett Electric Co. spokesman said a squirrel caused a short-circuit in a transformer. Charles Moran, the spokesman, said the squirrel got into a transformer at the Narragansett Electric's Dyer Street substation at 11:10am. Moran said a backup transformer took over automatically and prevented a power failure in downtown Providence. But "there was a slight power surge," he said.

Computers in the money-market divisions of the Fleet and Old Stone Banks

were down for half an hour after the power surge, but banking services were not disrupted, spokesmen said. Dean Witter Reynolds Inc., a brokerage firm, had trouble getting quotes on stock prices, according to Sharon Tallman, who said some of the firm's Quotron machines went down. At Superior Court, the computer was down for two hours, but it didn't affect court scheduling, a spokeman said.

"The mainframe on our IBM computer was down for over an hour," said Robert Perreira of the Providence Journal Co.'s computer services unit. Perreira said 14 systems went down and "three of them did not come up immediately." A Journal Co. electrician said the power surge caused "our lightning control panel to behave like a runaway monster." It caused a computer to activate a program designed to save energy on weekends by shutting off the lights in part of the building. "The computer thinks it's Sunday," the electrician said.

[A similar squirrelcide happened at SRI a while back. The side-effects were quite prolonged and unanticipated. On occasional Saturdays for several months all of SRI was powerless while repairs were repeatedly attempted but not quite completely accomplished. PGN]

Collision avoidance systems - FAA vs. Honeywell

<churd@labs-b.bbn.com>
31 Oct 86 11:01:30 EST (Fri)

A few months ago, Sixty Minutes ran an episode about the fact that the FAA had rejected Honeywell's collision avoidance system in favor of its own (untested, uncompleted) system. I think the episode aired shortly after the Air Mexico collision in California. One of the people Sixty Minutes interviewed had been an FAA official (executive?) until he became too vocal about the fact that the FAA was ignoring a workable system. It was his opinion that *many* collisions and near-misses would never have happened if the Honeywell system had been adopted when it was first introduced.

The Honeywell system resides in the aircraft and projects an envelope ahead of the plane that can be detected by another Honeywell system. The system communicates with the pilot by issuing a warning when an intersection with another plane's envelope is detected and gives a direction in which to turn to avoid collision.

The FAA system is tied into the ground-control system and seems to rely on tracking aircraft from radar on the ground. I was not too clear on this.

The advantage of the Honeywell system is that it is small, cheap, and does not require the pilot to rely on any outside assistance. The drawback is that *all* planes need to be equipped with the system. But, since it is small and cheap that would not be a great problem.

I can't remember all the pros and cons of the FAA system, but the cons had a clear majority. The system is much more complicated, involves ground-control personnel notifying pilots about impending collisions, and is expensive.

Charlie Hurd

The Military and Automatic Humans

Ronald J Wanttaja <nike!caip!uw-beaver!ssc-vax!wanttaja@cad.Berkeley.EDU>
Wed, 29 Oct 86 09:49:53 pst

After graduating about ten years ago, I entered the Air Force as a Satellite Systems Engineer. I was assigned to a unit operating a particular NORAD satellite system...no names, no mission statements, please. A buddy DID almost start World War III one night, though.

My job was real-time and non-real-time analysis of mission data from the spacecraft; the end result of my analysis was to advice the NORAD Senior Director of the validity of the data. A lot of factors had to be incorporated in my analysis...in "N" seconds, I had to take into account which spacecraft had reported, its health and status, DEFCON level, and "numerous other mission critical elements." Nudge, nudge...

Anyway, the job was highly dependent upon the experience of the analyst, as well as his intuition...we had to have a FEEL for what was right.

Three years after I joined the squadron, the unit was reassigned from the Aerospace Defense Command (ADCOM) to the Strategic Air Command (SAC). Now, SAC is the largest producer of automatic humans in the free world. In a word, SAC is checklist crazy...every task is broken down to the largest number of subtasks.

SAC treats its checklists as a way to eliminate the human element. Training two people to work as a team is unecessary...all they have to be able to do is call off the proper steps from the checklist. SAC uses simulators to allow its people to practice every step, and to handle every contingency. For instance, a missile launch officer has gone through the launch procedure in the simulator dozens of times before he is placed in an actual control room. The opening sequence in WAR GAMES is an example of what SAC is trying to avoid: The crew must automatically perform its tasks, spending no time thinking about what the consequences are. The crew must not bring their emotions into play, nor even any additional knowledge they must have. Every action must be governed by a checklist step.

You can see what our problem was...how to you place "intuition" and "gut feel" onto a checklist? Our job could not be performed by an automaton; we had to call on experience and a deep understanding of system operation in order to provide our assessment. We argued, to no avail. We had to have a checklist. So we thought and thought, and broke the analysis task into as many subelements as we could. The last subelement was OPERATOR INTUITION.

Did SAC complain? Nahhhhh...they never read the thing. Occasionally they'd show up for Operational Readiness Inspections. During the simulation, their checklist called for them to verify that we had our EVENT ASSESSMENT checklist open. Their checklist didn't call for them to actually read our checklists...

Assessing system effectiveness

"Scott E. Preece" <preece%mycroft@GSWD-VMS.ARPA>
Fri, 31 Oct 86 10:01:55 CST

> [Dave Benson said that we should assume that an overloaded system will fail to handle any load at all. I said an overloaded system could fail by handling no load, by handling its ceiling load and no more, or by handling its ceiling load and some decreasing part of additional traffic, and that we had no grounds for making that decision until a design, designers, and implementors existed. Dave Benson said history tells us no system works without extensive realistic testing.]

If that summary sounds as if I thought Dave's remarks didn't address what I said, that's correct. I know of systems (not military systems, with which I have have no experience) which demonstrate each of those overload behaviors; I'm sure he does, too. Overload behavior is something that certainly can be stated explicitly as part of the design and it's generally a pretty easy thing to simulate, compared with the problem of simulating all possible inputs. Note that I am talking ONLY about response to overload, which is where the discussion started.

I have plenty of doubts about many parts of the SDI program and I don't for a minute expect that they will come up with a design or an implementation that I will be willing to trust. But Dave's original statement that "We should assume that a system capable of handling N targets/sec will, when presented with 2N targets, fail to handle any at all." is without basis and his further statements referring to 30 years of software development history offer nothing to support it. Systems fail in many ways and there is no reason to assume a particular failure mode without looking at the design and implementation. Worst-case assumptions are often useful, but in this case they are unenlightening; we all know that in the worst case nothing works, all the missiles fall through, and c'est ca. I'm a lot more interested in the probability of that worst case than in the fact that that IS the worst case. Dave did not say anything to convince me that an arbitrary system's most likely response to overload is total failure; in my own experience (admittedly only 20 years) more systems respond to overload with degraded or limited performance than with total failure.

scott preece gould/csd - urbana
uucp: ihnp4!uiucdcs!ccvaxa!preece

Computers in elections

Jekyll's Revenge 264-7759 MKO1-2/E02 <hyde%abacus.DEC@decwrl.DEC.COM>
Friday, 31 Oct 1986 11:32:53-PST

The latest issue of DATAMATION has an excellent article on computerized vote counting. I recommend it to all. It addresses problems with punch card

voting, but doesn't address the problems with computerized voting booths. The three biggest problems with computerized voting booths are secrecy of internal operation, lack of recount capability, and inability for the voters to ensure that the computer votes as instructed. Some of the people whose names are in the article were at BU in August for the Symposium on Security and Reliability of Computers in the Electoral Process. These people are doing great work, especially considering the fact that they are generally financing it on their own.

I am presently compiling some poll watching guidelines for computerized elections. I can send a copy to anyone who will be a poll watcher on Tuesday.

17th FAULT-TOLERANT COMPUTING SYMPOSIUM

Flaviu Cristian <FLAVIU@ibm.com>
29 October 1986, 09:54:36 PST

[Remembering that the RISKS Forum is aimed at fostering better systems in the future as well as exposing limitations with existing systems, it is appropriate to include the following item. PGN]

CALL FOR PAPERS
FTCS17
THE SEVENTEENTH INTERNATIONAL SYMPOSIUM
ON FAULT-TOLERANT COMPUTING
sponsored by IEEE Computer Society's Technical
Committee on Fault-Tolerant Computing
Pittsburgh, PA, July 6-8, 1987
**** NOTE NEW DATES ****

The Fault-Tolerant Computing Symposium has, since 1971, become the most important forum for discussion of the state-of-the-art in fault-tolerant computing. It addresses all aspects of specifying, designing, modeling, implementing, testing, diagnosing and evaluating dependable and fault-tolerant computing systems and their components. A special theme of the conference will be the practical application of fault-tolerance to the design of safety critical systems, real-time systems, switching systems and transaction systems.

Papers relating to the following areas are invited:

a) design methods, algorithms for distributed fault-tolerant software systems,

b) specification, design, testing, verification of reliable software,

c) specification, design, testing, verification, diagnosis of reliable hardware

d) fault-tolerant hardware system design and architecture,

e) reliability, availability, safety modeling and measurements,

f) fault-tolerant computing systems for safe process control, digital

switching, manufacturing automation, and on-line transaction processing.

Authors should submit 6 copies of papers before the submission deadline December 5, 1986 to the program co-chairmen: Flaviu Cristian, IBM Research K55/801, 650 Harry Rd., San Jose, Ca 95120-6099, USA, and Jack Goldberg, SRI International, 333 Ravenswood Ave., Menlo Park, Ca 94025. Papers in areas a, b, and f should be sent to F. Cristian, and papers in areas c, d, and e to J. Goldberg.

Papers should be no longer than 5000 words, should include a clear description of the problem being discussed, comparisons with extant work, and a section on major original contributions. The front page should include a contact author's complete mailing address, telephone number and net address (if available), and should clearly indicate the paper's word count and the area to which the paper is submitted. Submissions arriving late or departing from these guidelines risk rejection without consideration of their merits.

The Symposium chair and vice-chair are John Shen and Dan Siewiorek, both from Carnegie Mellon University, USA. The program co-chairmen are: Flaviu Cristian, IBM Research, USA, and Jack Goldberg, SRI International, USA. Publicity chairman is Bella Bose, Oregon State Univ., USA.

[Program Committee omitted here.]

Search RISKS using swish-e

THE RISKS DIGEST

Forum on Risks to the Public in Computers and Related Systems

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

Volume 4: Issue 3

Monday, 3 November 1986

Contents

The Big Bang at the London Stock Exchange

Jonathan Bowen <bowen%sevax.prg.oxford.ac.uk@Cs.Ucl.AC.UK>
Tue, 28 Oct 86 17:24:41 GMT

Headlines in `The Independent' (new British `serious' newspaper) on Tuesday 28 October 1986:

> Stock Exchange computers fail under strain
> Shambles as the Big Bang hits the floor

THE CITY'S "Big Bang" exploded after just 29 minutes' trading yesterday morning when the computers buckled under the strain. The Stock Exchange system which speads information to dealers and investors went off the air at 8.29 am, to be followed 18 minutes later by the central dealing computer, the Stock Exchange Automated Quotations system known as SEAQ. By that time, market makers were already experiencing problems in putting their prices into the system, and some of them had ceased to trade at all. The failures were blamed by the Stock Exchange on brokers overloading the system, both to look at their competitors prices and out of pure curiosity.

Jonathan Bowen, Programming Research Group, Oxford University

---

UK computer security audit

Robert Stroud <robert%kelpie.newcastle.ac.uk@Cs.Ucl.AC.UK>
Thu, 30 Oct 86 12:27:45 gmt

There was an item in today's Independent (a new UK paper) about the results of a security audit of 50 UK companies. Sadly, the results will be all too familiar to RISKS readers. When will practice catch up with theory?

Robert Stroud, Computing Laboratory, University of Newcastle upon Tyne.
UUCP ...!ukc!cheviot!robert

[Sorry for the absence of a specific reference to the original report. PGN]
["It is probably one of those expensive management consultancy things costing ten pounds a page!" - Robert]

==========

Reproduced without permission from The Independent 30th October 1986 p.16

"How Fred lets the fraudsters in" (c) Newspaper Publishing PLC
by Michael Cross

Frauds involving computers will cost British companies 40m pounds next year, the insurance broker Hogg Robinson said yesterday. The culprits are not usually teenage computer wizards but disgruntled employees and previous employees.

Hogg Robinson's report, an audit of 50 firms, suggests that British companies are extraordinarily careless about looking after their computers. Apart from fraud, the dangers are sabotage, damage caused by carelessness, and run of the mill disasters such as fire or flood.

The chink in most computers' armour is the password. All but three sites the auditors examined used passwords to control access to computers. Most were useless. When people choose their passwords, they often pick names of spouses or pets. These are easy for colleagues to guess. America's favourite password is "love", closely followed by "sex". Top of the list in Britain is "Fred".

Other favourites, said David Davis, director of research at Hogg Robinson, are "pass", "God", "genius" and "hacker". "If a hacker tries these he will get through 20 per cent of the time", Mr Davis said.

Passwords are particularly vulnerable when they remain unchanged for a long time. The chairman of one major company the auditors investigated had kept the same password for five years. It was "chairman".

Another danger point is in computers that allow unlimited guesses at passwords. One in 10 of the sites surveyed allowed any number of attempts to "log in". The really secure passwords are the dual-key encrypted type. These are codes distributed in two parts, which link up inside a computer. But only two or three computers, all government installations, carry such protection in Britain.

Despite the vulnerability of passwords, the report suggests that few computers fall victim to outside "hackers". Three of the sites inspected showed signs that hackers had gained access to the computers through external telephone lines. Dr Frank Taylor, chairman of the British Computer Society's security committee, said there is no real evidence that hackers are causing large financial losses.

Dr Taylor's horror stories have a more humdrum flavour. One concerns a building supplies company which had no security on its counter terminals. Crooked employees were able to give huge discounts to friends, and the company went broke. Another company lost its data - and nearly everything else - when lightning struck a power cable.

Computers face a host of dangers from everyday activities, the report says. Mr Davis said that computers are designed to be operated by, "a race of supermen who do not eat, drink or smoke". He has a useful tip for computer people who cannot give up human habits; drink black coffee rather than white. It causes less damage if spilt.

Austin's computer-controlled traffic lights

Alan Wexelblat <wex@mcc.com>
Mon, 3 Nov 86 13:07:27 CST

A while back I reported that a lighning strike had taken out the computer that controlled the synchronization of Austin's downtown traffic lights. (Local control units took over - only two lights went "on the blink".)

I recently learned that there was more to the story. It seems that Austin has a "traffic flow program" embedded in that system that changes the durations of red/yellow/green lights for given intersections based on the time of day. The goal is to give more time for people to get intown in the mornings and out of town in the evening. The local control units fall back to an "equal time for all" scheme, regardless of time of day.

Since the power loss occurred late in the afternoon, evening rush hour traffic was snarled more than usual. In addition, there were several near-accidents caused by people who "knew" that the yellow light would be long enough (based on months of commuting experience).

Alan Wexelblat
UUCP: {seismo, harvard, gatech, pyramid, &c.}!ut-sally!im4u!milano!wex

---

Computers and Medical Charts

Elliott S. Frank <amdahl!esf00@decwrl.DEC.COM>
Mon, 3 Nov 86 12:44:14 PST

The following items were posted to the delphi digest on mod.mac. The issues have been covered before in mod.risks, but the example is worth noting.

Elliott S Frank ...!{ihnp4,hplabs,amd,nsc}!amdahl!esf00 (408) 746-6384

==========

Delphi Mac Digest Thursday, 30 October 1986 Volume 2 : Issue 55
From: PIZZAMAN (14213)
Subject: Computers and Medical Charts
Date: 26-OCT 16:26 Business Mac

The most amazing thing happened at the hospital yesterday. I was accused of unethical behavior because I used my computer to prepare a conference for the Department of Surgery!

Let me explain.... I am the Clinical Coordinator of the Department of Surgery at a rural community hospital. This is a voluntary job, in addition to my regular practice of surgery. My responsibilities include the preparing of the mortality and morbidity conferences each month, as well as trying to put together educational topics of interest for the other surgeons. Having trained at a University Hospital in Philadelphia, I enjoy doing this teaching.

In order to prepare for one of these conferences, I took my Tandy 100 to the record room, and took my notes on it. When I got to the office, I plugged the Imagewriter cable into the RS-232 connector on the back of the Tandy, and using Smartcom II, loaded the information into the Mac for work processing, spread sheeting, and graph creation.

Now, I am being accused of taking confidential information out of the hospital in the form of patient records and doctors names! All I had on the computer were my notes. The paranoid medical staff is afraid that having this information in my "COMPUTER" is dangerous, in some way. Since I consider my two computers just extensions of other work tools that I use, I can't understand this. Would they be just as paranoid if I used a legal pad to make notes instead of the computer?

By the way, the bylaws of the hospital allow for the use of records for research, and I had permission from the President of the Medical Staff to do the study in question.

Pretty amazing paranoia, huh? Do people really still fear computers this way? Any physicians out there have similar experiences? Any legal advice?

==========

From: PEABO (14226)
Subject: RE: Computers and Medical Charts (Re: Msg 14213)
Date: 26-OCT 19:45 Business Mac

It might have something to do with Legislators, who tend to know even less about computers than hospital staff. I've read some stories about how some corporations are getting concerned about what J. Q. Middlemanager is taking home to work on using his own computer after downloading from the company mainframe.

peter

==========

From: LAMG (14239)
Subject: RE: Computers and Medical Charts (Re: Msg 14213)
Date: 27-OCT 01:20 Business Mac

Yes, it's paranoid behavior, but no, it's not amazing, I'm afraid. In my institution (UCLA Dept. of Radiological Sciences) most of the data used for teaching and research is in "machine readable" form at one time or another. Clearly there is a valid issue related to the removal of confidential patient records from the hospital (I don't know what the regulations are there) but these would apply equally to data whether in handwritten, printed or machine readable form.

You didn't say exactly who is objecting to your work and on what grounds, but it sounds like they don't have a very good idea of what you're using the computers for. I can't give you legal advice though.

Franklin Tessler, M.D.

Search RISKS using swish-e

Report problems with the web pages to the maintainer

Search RISKS using swish-e

THE RISKS DIGEST

Forum on Risks to the Public in Computers and Related Systems

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

Volume 4: Issue 4

Tuesday, 4 November 1986

Contents

Flawed Radars in Air Traffic Control

Peter G. Neumann <Neumann@CSL.SRI.COM>
Tue 4 Nov 86 09:55:22-PST

FAA Says It Has Fixed Flawed Radar Systems

Santa Ana (UPI, 4 Nov 86; from the San Francisco Chronicle of that date, p. 40)

Malfunctions in key radar systems that track airliners in Southern California reached a hazardous level in recent years, but officials said yesterday that the most serious problems have been found and fixed. According to Federal Aviation Administration reports obtained by the Orange County Register, there were frequent breakdowns in the past four years in the Laguna Radar, which monitors the area in a 200-mile radius around its perch east of San Diego, and the San Pedro Radar, which scans a 200-mile circle around the Palos Verdes Peninsula. The systems monitor air traffic for Los Angeles International Airport, John Wayne Airport and Lindbergh Field in San Diego.

The radar malfunctions grew critical enough that the FAA sent tecnicians from Washington, D.C., to the Air Route Traffic Control Center in Palmdale two weeks ago to monitor both systems and make adjustments. Among the malfunctions were frequent disappearances of airplanes from radar screens for 15 to 30 minutes and radar displays that show planes in a turn pattern when they are actually on a straight course.

In some instances, the Register reported, air controllers saw aircraft "jump" on their radar scopes, which made planes appear to have changed

direction when they had not. In others, radars tracking plane descents in an especially busy corridor showed jets traveling faster than they actually were. In addition, important altitude data that helps controllers avoid midair collisions frequently disappeared from radar screens.

FAA official Russell Park confirmed the problem and acknowledged that the situtation could have been hazardous. He said the malfunctions played no part in any collisions, including that of an Aeromexico DC-9 and a small plane over Cerritos on August 31. He said the troubleshooting team from Washington was able to fix the most serious malfunctions quickly.

[Quickly? But this went on for FOUR YEARS? PGN]

[By the way, the November 1986 issue of the IEEE SPECTRUM is devoted to "Our Burdened Skies", and is a goldmine for those of you interested in our air transportation system.]

The Future of English (risks of technocrats, risks of word processors)

Martin Minow, DECtalk Engineering, ML3-1/U47 223-9922 <minow%regent.DEC@decwrl.DEC.COM> 29-Oct-1986 1645

[Prediction]
THE FUTURE OF LANGUAGE

[By Anthony Burgess. From "2020: A Vision of the Future," in the 17 June 1986 "London Telegraph Sunday Magazine," a special issue devoted to the future. Burgess is the author of "A Clockwork Orange," "Earthly Powers," "Napoleon Symphony," "Nineteen Eighty-Five," "Re Joyce," and many other books.]

Prime ministers speaking to the nation still attempt, like Mrs. Thatcher, to use "Standard English" and a supraregional or classless accent. By 2020 they will not have to do that. What they will have to do is speak a kind of English that denies the fact of education, avoids allusion to Shakespeare or the Bible, and, where it rises above the level of conversational usage, gains a pose of learning and authority from the use of technological terms. At the same time, with a kind of ultimate authority seeming to be vested in the hard but high-flown language of science, there will be more mendacity and evasion dressed up as technology. The Pentagon has already shown the way with such expressions as "anticipatory retaliation," which does not sound like striking the enemy without due declaration of war.

America's language is already far advanced in the direction of combining the loose colloquial with the cant terms of the technical specialists -- who include sociologists and psychologists, as well as cybernetics experts and aerospace men. When not being expertly evasive ("at this time the nuclear capability of this nation is not anticipated to assume a role of preemptive preparatory action"), it is slangy, unlearned, unwitty, inelegant. At its most disconcerting it combines two modes of discourse: "Now we zero in on the nitty-gritty of the suprasegmental prosodic feature and find that we're into a different ball game." It is already, perhaps, the matrix of British English of 2020.

As for the sound of the English of 2020, some of its characteristics are in active preparation. Assimilation -- a natural enough process, which, however, must never be allowed to go too far -- is drawing a lot of vowels to the middle of the mouth, where the phoneme called schwa (the second syllable of "butter," "father;" the first a in "apart") waits like a spider for flies. The "a" of "man" is already a muzzy, neuter sound with the young. Assimilation of consonants is giving us "corm beef: and "tim peaches" and "vogka" (Kingsly Amis spotted these in the early seventies). Grammar has been simplified, so that most sentences are constructed to the "and...and...and..." Biblical formula (hypotactic, to be technical). Losing Latin in our schools, we are finding it hard to understand Milton and to appreciate the beauties of the periodic sentence.

This will get worse. The English of 2020 will combine structural infantilism with hard-nosed technology. It will be harsh, and it will lack both modesty and humor.

The written word is only a ghost without the solidity of the spoken word to give it substance, but to many it seems to be the primary reality. After all, the voices of dead poets and novelists survive only as black marks on white paper. Still, writers write well only when they listen to what they are writing -- either on magnetic tape or in the auditorium set silently in their skulls. But more and more writers -- not only of pseudoliterature but of political speeches -- ignore the claims of the voice and ear.

I think that, with the increasing use of the word processor, the separation of the word as sound from the word as visual symbol is likely to grow. The magical reality has become the set of signs glowing on a screen: this takes precedence over any possible auditory significance. The speed with which words can be set down with such an apparatus (as also with the electric typewriter), the total lack of muscular effort involved -- these turn writing into a curiously nonphysical activity, in which there is no manual analogue to the process of breathing out, using the tongue, lips, and teeth, and accepting language as a bodily exercise that expends energy.

What is wrong with most writing today is its flaccidity, its lack of pleasure in the manipulation of sounds and pauses. The written word is becoming inert. One dreads to think what is will be like in 2020.

I have never yet ventured a prophecy that came true. In my little novel "Nineteen Eighty-Five" I get nothing except the name of the son of the Prince of Wales. It is altogether possible that, rejecting the easy way of pop music, drugs, and television, the youthy of the near future will stage a reactionary revolution and go back to Latin, Shakespeare, and the Bible and insist on school courses in rhetoric. But I do not think it likely.

[It should be noted, perhaps, that the Boston Globe recently published an article that stated the offering of Latin in public high schools has increased markedly in the last five years. MM]

Burgess notes that word processors make writing too easy. You can see the result in the bloated junk novels, all over 300 pages long, that seem to be designed only to fill waiting time at airports.

One of my colleagues once edited a computer textbook written by one of the more important educators in the field (and he is a well-known writer himself). He said that "he nearly wore out the delete-paragraph key on the word-processor." The bad news is that there seems to be no real interest in good editing in the commercial marketplace. I would claim that this is a direct result of the ease of writing with word processors.

Martin

[In a recent memo, EWD976-0, 10 Sep 86, Edsger W. Dijkstra makes a plea against bad writing. One of his suggestions for making it easier on your readers was this: ``Avoid if possible using one-letter identifiers that are all by themselves words in the language of the surrounding prose, such as "U" in Dutch and "a" and "I" in English, as they may confront you with unpleasant surprises. (There is a page by David Gries, in which "I" occurs in three different roles: as a personal pronoun, as identifier for an invariant and as a Roman numeral! Of course, the reader can sort this confusion out, but it is better avoided.)'' EWD via PGN]

Search RISKS using swish-e

THE RISKS DIGEST

Forum on Risks to the Public in Computers and Related Systems

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

Volume 4: Issue 5

Wednesday, 5 November 1986

Contents

Computer causes chaos in Brazilian Election

Jonathan Bowen <bowen%sevax.prg.oxford.ac.uk@Cs.Ucl.AC.UK>
Tue, 4 Nov 86 15:23:54 GMT

From Daily Telegraph, Monday November 3rd:

``Hundreds of thousands of Brazilians may not be able to vote in the forthcoming general election because of bureacratic bungles. ... only 70% of the electorate have been issued with the essential voting card. .... queues and frayed tempers are a result of a 30 million pound [c $42 million] computerisation programme which was designed to streamline voting and eliminate fraud. ... Flaws in the system only became evident when distribution started three weeks ago. ... [the computer] has been programmed to cancel all duplicate applications in order to weed out fraudulent "phantom" voters. ... while it showed that 1,400 dead people had voted for the mayor in the north-eastern town of Teresinha last year, and 100,000 falsified cards were in circulation in the southern state of Santa Catarina, it also cancelled legitimate names. Programmers overlooked that twins are born on the same day to the same parents. Consequently, the voting rights of an estimated 70,000 twins were cancelled. The Federal Electoral Tribunal in Brasilia is currently

wading through 140,000 appeals, including the case of a certain Jose Francisco, who says all his 14 brothers were baptised with identical names. ... It is hoped that all those eligible will have their cards by the 15th. Those that do not will have to pay a 4 pound [c $5.50] fine or brave more queues and bureacracy to prove that they both exist and have the right to vote.''

Surely these sorts of problems have occurred before in other countries. What methods are available, if any, the avoid such risks using computers without human intervention? Are such problems a result of there not being *enough* computerised information on the population to start with?

Risks of FAA Philosophy ?

Robert DiCamillo <rdicamil@cc2.bbn.com>
Wed, 5 Nov 86 16:18:19 EST

The recent entries in the Risks Journal about collision avoidance systems reminds me of a comment a professor once made to me about the philosophy of the FAA. For many years this professor in the Engineering Design Department at Tufts University worked on a better engineered cockpit layout and display system. This included improvements in human factoring, multi-function graphic displays to eliminate the number of indicators needed, and more functionality in the cockpit to allow the pilot to detect and avoid other aircraft.

After several years of work, where along the way many graduate students had also contributed, the system was presented to the FAA and turned down for what the inventors could not fathom as valid technical reasons. The system was better, easier to use, and provided the pilot with more functionality and autonomy over his aircraft and flight path.

The professor noted that the catch was the FAA's "apparent" philosophy that they don't want the pilots to have more autonomy in determining their flight path and collision avoidance, as this task is considered the realm of the ground (air traffic) controllers. His opinion was that any system that included decentralization from ground control would be rejected because the FAA does not want to threaten the job security of air traffic controllers.

This political "unspoken" philosophy of the FAA would still seem to be in effect, providing you are willing to believe that technical reasons (good or bad) will be used to defend such political objective(s). Perhaps the Honeywell System is just another casualty.

This of course leads to the question of policy making. Does anyone know if the FAA charter contains any such implicit endorsement pro or con relative to evaluating technology ? Does the FAA even have an agreed upon philosophy in this regard that is published and accessible to the public ? Or does some high ranking, politically inclined, individual have the absolute veto power within the government (FAA or otherwise) ?

This seems like one of those issues that will be difficult to substantiate,

most suitable to think about while flying in planes. Note that the November 1986 issue of the IEEE Spectrum is devoted to "Our Burdened Skies". Although I haven't read it yet, I will be interested to see if there is any reflection (real or ghost) of such an FAA philosophy.

- Robert DiCamillo

Computers and Medical Charts

Christopher C. Stacy <CSTACY@JASPER.Palladian.COM>
Wed, 5 Nov 86 21:33 EST

I talked to an R.R.A. today to get an opinion on PIZZAMAN's story about taking the medical records information home on his computer.

The hospital sets up regulations to control access to the medical records, which are carefully guarded as sensitive confidential information. The physical record is considered to be owned by the hospital, and the information is considered to be owned by the patient. Typically, physicians are allowed to take copies of medical records to their offices or home in order to perform work directly related to patient care. Preparing research reports is generally considered to be within that scope.

People are generally not allowed to remove the original physical record from the hospital, but copies may be OK. The administrator I talked to didn't think that it was significant that the information was copied using a computer. Of course, the physician has a serious responsibility to protect the information from perusal by random persons, including his family, visitors to his office, people logging in to his computer over the phone, etc.

So, the opinion of one medical records administrator seems to concur with that of Dr. Tessler; the people at that hospital probably were over-reacting inappropriately.

I don't know how well most medical personnel understand what computers are; the person I talked to currently works for a company that writes software for hospital administration.

So, this situation presents the familiar risk of paranoid confusion. However, I would identify the major risk here as related to computer and telecommunications security. This is the same concern as for the hospital which keeps their actual medical records online. The two risks can be related, of course.

If people have other questions or thoughts about this, I would be glad to forward them along to my friend; she was interested that people were discussing this sort of thing.

Re: Insurgent Squirrel Joins No-Ways Arc

Wombat <rsk@j.cc.purdue.edu>

Wed, 5 Nov 86 21:31:22 EST

Ross's story reminds me of a similar incident which took place at Purdue about five years ago; a misplaced rodent [in a power transformer] caused most of the campus to lose power for about half a day. The university physical plant crews actually aggravated the situation while trying to fix it by mis-diagnosing the trouble, in ways that have never been clear. One of the physical plant officials was quoted on the front page of the Exponent (Purdue's daily) as saying "You've got to understand, with electricity you never quite know what's going on". I'm sure he was thrilled when a group of EE students reprinted that quote on T-shirts and proceeded to sell them at a brisk pace for the rest of the semester. [I still wear mine!]

Rich Kulawiec, rsk@j.cc.purdue.edu

Micros in Car engines

Peter Stokes <stokes%cmc.cdn%ubc.csnet@CSNET-RELAY.ARPA>
Wed, 5 Nov 86 11:46:07 pst

My 1986 Ford Mustang has (according to the literature) a micro-processor controlled engine. When driving it, you can tell that the engine RPM's are contolled by something "intelligent" :

- the high idle when cold to normal idle when warm transition has a distinctive change sequence as the engine warms up and this response is IDENTICAL every morning as I drive to work.

- If you hit the accelerator pedal and let go quickly, the engine speed returns to normal in about 3 distinctive steps:
  1: a sharp drop of several hundred RPM's,
  2: a smoother drop to very near the idle speed, and finally,
  3: a small adjustment to the true idle speed.

- If you disengage the clutch while the car is moving (first step in gearing down), the engine speed drops quickly to a low of 200 RPM's (I can sometimes feel it shudder) and then the processor corrects this with a "shot of gas". If you leave your foot on the clutch and just coast, you can observe the tachometer settle on the idle speed after a small amount of overshoot and undershoot.

- and finally, if you try to stall the car (starting off in first gear without pushing the gas for example), the processor responds by trying to keep the engine speed at idle speed.

My Question... What are the risks in buying and driving an automobile with a computer controlled engine?

Safety: What are the odds of a malfunction causing acceleration?
Performance: Is this a feature? Will the benefits of the microprocessor control continue to serve as the engine grows old and changes?
Service: Can a "Saturday Morning Mechanic" still tune his/her car or

is specialized equipment now a pre-requisite for the job?
Safety: Can the control over the engine be affected by an external source (e.g. radio transmitter)? I have noticed erratic engine idle while in an automatic car wash....

Peter Stokes
Envoy100: cmc.vlsiic (...usual disclaimer...)
CDNnet: stokes@cmc.cdn
BITNET: stokes@qucdncmc.bitnet

[...probably not much risk in BUYING one, but DRIVING ONE is another matter. Since you probably do not read every line of RISKS, let me remind you of the following cases, summarized in RISKS-4.1. (The Mercedes case was noted in RISKS-2.12.) PGN]

AUTOMOBILES:
Mercedes 500SE with graceful-stop no-skid brake computer left 368-foot skid marks; passenger killed (SEN 10 3)
Sudden auto acceleration due to interference from CB transmitter (SEN 11 1);
Microprocessors in 1.4M Fords, 100K Audis, 350K Nissans, 400K Alliances/ Encores, 140K Cressidas under investigation (SEN 10 3)
El Dorado brake computer bug caused recall of that model [1979] (SEN 4 4)
Ford Mark VII wiring fires: flaw in computerized air suspension (SEN 10 3)


Search RISKS using swish-e

Report problems with the web pages to the maintainer

Search RISKS using swish-e

THE RISKS DIGEST

Forum on Risks to the Public in Computers and Related Systems

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

Volume 4: Issue 6

Thursday, 6 November 1986

Contents

Computerized Reagan swamps Hospital with calls

Werner Uhrig <werner@ngp.utexas.edu>
Thu, 6 Nov 86 05:14:08 CST

[Wed 5 Nov 86 15:38]

In the San Diego Union was an article from the AP newswire. A tape recording of President Reagan urging voters to go out and vote Republican went haywire and continuously called phone lines at a hospital in Texas. Over a six hour period several of the hospital phone lines received a phone call every three minutes.

Aftermath of the Big Bang

Robert Stroud <robert%kelpie.newcastle.ac.uk@Cs.Ucl.AC.UK>
Thu, 6 Nov 86 16:51:48 gmt

Today (November 6th) is the first day that there has NOT been an item in my paper about some computer failure or other problem resulting from the Big Bang! Accordingly, it seems like a good time to take stock, and report what

has been going on. But first I would like to deal with a comment Jerry Saltzer made about my original posting.

I quoted a newspaper article which referred to the TOPIC terminal network used by the Stock Exchange as being

> . . . six years old and considered fairly antiquated by today's standards.

and Jerry Saltzer replied

> I wonder who it is that considers that system as antiquated? Another
> perspective says that a complex system that has been running for six
> years is just beginning to be seasoned enough that its users can have
> some confidence in it...

Well, it was Sir Nicholas Goodison, the chairman of the Stock Exchange who said that TOPIC was antiquated rather than a computer scientist, although perhaps he was influenced in this view by his technical staff. He was also quoted as "having breathed a sigh of relief" when he heard that the problems were only with TOPIC and not the brand new and expensive (18 million pounds?) SEAQ system. To its credit, as far as I know, SEAQ has not failed yet, although it has been taken out of service on several occasions when TOPIC has broken in the interests of fairness - some people can access SEAQ directly and this would give them an unfair advantage.

Anyway, TOPIC probably was very stable ("tried and trusted" was another phrase in the article I quoted) until the Stock Exchange started tinkering with it just before the Big Bang. Indeed, according to an article in Computing (Oct 30th), the Stock Exchange "opened an electronic gateway" allowing access to detailed SEAQ price information by an additional 7,500 screens at the last minute, effectively quadrupling the load. The rest is history.

As far as the technology being antiquated goes, I believe that TOPIC provides a video feed (Teletext) whereas SEAQ provides a digital feed, and perhaps it is significant that it was the TOPIC/SEAQ link that failed. Apparently, video is much less convenient for wiring up a dealing room so that you can switch information between desks flexibly.

So perhaps, in that limited sense TOPIC is indeed antiquated, but the real problem was caused by the tinkerers as Jerry said. However, I think that to some extent, the issue here is akin to the recent discussions about whether software rots. What changes are the assumptions a system makes about its environment, and the Big Bang certainly produced a radically new environment.

Anyway, back to what's been happening since last Monday (Big Bang day). TOPIC went down again on Tuesday at lunchtime, but since then has been reasonably well behaved thanks to various emergency measures designed to minimise the load. In particular, there are restrictions on the time of day that you can enter new pricing information, and the page refresh rate has been decreased. The Stock Exchange anticipated a 50% increase in demand, but the load actually doubled. The Sunday Times quoted the figure of 2.2 million page requests/day (as opposed to 500,000 on NASDAQ, a comparable system on Wall Street). Two new computers have been ordered to add to the eight which already support the network, and should increase the capacity by 50%. On

Monday, a malfunction replaced the British Aerospace share prices with those for Bass (a brewery).

But perhaps the most serious problem is the backlog of unmatched trade reports which will have to be sorted out before accounts can be settled. At the weekend, after one weeks trading, there were 55,000 such unmatched records, and even worse, despite working at it all weekend, only 2,000 were resolved. By Tuesday, there were at least another 4,000 bringing the total to 59,000 and 15 security firms are reported to be having difficulties with the new settlement system.

It is difficult to put these figures into perspective without knowing the total number of trades in a week. 55,000 seems pretty big to me, and is apparently five times the average, but then 11,000 also seems pretty big! A semi-informed guess would be that 55,000 represents about 30% of the weeks trading.

The main reason for the backlog is a power failure at a computer bureau last week, but human error caused by lack of familiarity with the new systems, and "insufficient decimal precision" have also been blamed.

So with nothing in the paper today, everything appears calm, but as the Independent put it yesterday, "behind the scenes, officials are faced with nightmarish problems". The next big test of the system will be in December when trading starts in 6 billion pounds worth of British Gas shares, the biggest share issue ever, aimed at getting as many share holders as possible, (7 million people have expressed an interest!). I think the dealers might just be going back to the deserted trading floor of the Stock Exchange...

[Sources: Computing, Sunday Times, Independent]

Robert Stroud, Computing Laboratory, University of Newcastle upon Tyne.
UUCP ...!ukc!cheviot!robert

Fault-tolerant-computer manufacturer RISKS

Robert Stroud <robert%kelpie.newcastle.ac.uk@Cs.Ucl.AC.UK>
Thu, 6 Nov 86 17:05:57 gmt

This is my favourite Big Bang story and comes from the not entirely serious Backbytes column of Computing (Oct 30th), reproduced without permission.

Robert Stroud, Computing Laboratory, University of Newcastle upon Tyne.
UUCP ...!ukc!cheviot!robert

"Dog days for dire Stratus" (c) Computing

As the blue touch paper for the Big Bang was finally lit this week, one company that must have allowed itself a sigh of relief is fault-tolerant computer manufacturer Stratus.

The trouble is that, while stockbroker companies are usually delighted with their Stratus machines, they [the companies] have an unfortunate

habit of demonstrating the non-stop capabilities to clients by wrenching out a circuit board while the computer is in operation.

Over recent months this habit has caused havoc at the UK customer assistance centre of Stratus in downtown Hounslow, Middlesex.

All Stratus computers sold in the UK are linked to the centre by autodial modem. In the case of any part apparently 'failing', red lights flash in the centre and the requisite replacement is hastily dispatched, complete with service engineer.

With the boom in fault-tolerant sales as financial institutions geared up for Big Bang, the 'cry wolf' situation began to get out of hand. Desperate engineers have now solved the problem by placing a timing delay in the alarm system to allow sticky fingered stockbrokers time to put the board back.

With computer-based dealing starting for real this week and keeping everyone in the financial institutions well occupied, Backbytes is sure that the problem will disappear anyway.

Re: Micros in Car engines

dw <Wegeng.Henr@Xerox.COM>
6 Nov 86 11:43:53 EST (Thursday)

My father once told me about a semi-truck that was being used to test an experimental microprocessor-controlled engine. Apparently the micro would crash (the computer, not the truck) whenever the truck was driven near the local airport. It was finally determined that the cause was EMI from a radar transmitter at the airport. Fortunately, when the micro crashed the engine simply died, although one can easily imagine worse consequences.

I'm told that they now test their experimental systems by simply driving them past the Voice of America transmitter near Cincinnati. If the system can operate under the conditions there, then they believe that it should operate almost anywhere!

/Don [A new definition of "exhaustive testing"? PGN]

The required redundancy/diversity can be and is achieved for software and for hardware, e.g.:

In nuclear reactor systems the redundant data processing systems -- old fashioned hardwired systems as well as computerised systems -- are in redundant, strictly separated rooms, sometimes even different parts of the building. The same applies for the cabling, which is routed different ways ASAP from the instrumentation points. (This is at least true for current reactors in Germany.) If redundant software is developed using design

diversity or n-version-programming properly, in connection with a certain amount of robustness and checking involved, not all versions will always suffer the same way from some strange events. The more you know about these events, the more you can do about it and make your system more fault-tolerant.

Udo Voges, Kernforschungszentrum Karlsruhe, idt766@dkakfk3.bitnet

Search RISKS using swish-e

THE RISKS DIGEST

Forum on Risks to the Public in Computers and Related Systems

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

Index to Volume 3

Sunday, 2 November 1986

THE RISKS DIGEST

Forum On Risks To The Public In Computers And Related Systems

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

Search RISKS using swish-e

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

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

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

Feeds

RSS 1.0 (full text)

RSS 2.0 (full text)

ATOM (full text)

RDF feed

WAP (latest issue)

Simplified (latest issue)

Smartphone (latest issue)
Under Development!!

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

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

Selectors for locating a particular issue from a volume

Volume number: Volume Issue Number: Issue

Get Specific Issue

Volume Index

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

Index to the RISKS Digest

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

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

Search RISKS using swish-e

THE RISKS DIGEST

Forum on Risks to the Public in Computers and Related Systems

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

Index to Volume 5

Thursday, 31 December 1987

Forum on Risks to the Public in Computers and Related Systems

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

Full Body Scan and pat down in progress

You were warned....

Search RISKS using swish-e

THE RISKS DIGEST

Forum on Risks to the Public in Computers and Related Systems

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

Volume 3: Issue 89

Tuesday, 28 October 1986

Contents

Airplanes and risks

Alan Wexelblat <wex@mcc.com>
Tue, 28 Oct 86 11:23:52 CST

Today's paper has a couple of airplane-related items that got me to thinking.

One item is a story on how the FAA is going to adopt strict rules for small aircraft in busy airspaces and establish a system to find an punish pilots who violate these rules. The question this brought to mind is: is this the right approach for the FAA's problem? How about for computer systems? Can (or should) we manipulate the user so that he uses the system the way we designers intended it to be used? Is training the answer (as suggested by the Navy emergency stories)?

The next item is an analysis of the emergency aboard the Thai jet. Apparently the fault is similar to the one that doomed the JAL 747 that crashed recently in Japan. The factor that made the difference -- according to Hiroshi Fujiwara who is deputy chief investigator of Japan's Aviation Accident Investigation Commission -- was that the Thai Airbus A-300 retained hydraulic control of the flaps and rudder on the tail.

Both the 747 and the A-300 have triply-redundant hydraulic systems, but on the 747 all three pass through the rear bulkhead in the same opening. Thus all three were ruptured at once. On the A-300 there are three separate openings and while two of the systems were ruptured in the Thai jet, the third remained usable.

The related question is: can we make use of this feature in computer systems (hardware or software)? That is, if a program has three ways of doing something can we isolate them so that a bug somewhere doesn't simultaneously cripple all three? Can we (given needs like security) separate computer hardware so that it is much more difficult to simultaneously destroy primary and backup hardware?

Comments and discussion welcomed.

Alan Wexelblat
ARPA: WEX@MCC.ARPA or WEX@MCC.COM
UUCP: {seismo, harvard, gatech, pyramid, &c.}!ut-sally!im4u!milano!wex

---

TSE, Air Canada

<Matthew_Kruk%UBC.MAILNET@MIT-MULTICS.ARPA>
Mon, 27 Oct 86 10:46:30 PST

No doubt you will hear more about these items from better informed sources. I merely heard brief summaries on the morning news today (Monday, 27th).

1. The Toronto Stock Exchange computer went down for about 5 minutes this morning. No cause given (yet).

2. A fire in a building, which houses the main computer (reservations?) of Air Canada, in Montreal. An Air Canada official cannot predict the effect on people holding advance registration. Damage cost estimates run in the millions.

Presumably there will be more information in tonight's paper. I'll try to get a summary out as soon as I can.

Big Bang [Also noted by Martin Minow. Thanks.]

Robert Stroud <robert%kelpie.newcastle.ac.uk@Cs.Ucl.AC.UK>
Tue, 28 Oct 86 19:42:40 gmt

Yesterday, October 27th, was the day of the Big Bang in the City - a revolution in the way in which the Stock Exchange is organised. Basically, three things happened - the market was opened to foreigners, the distinction between jobbers (who trade on their own account) and brokers (who buy and sell on behalf of clients) was abolished (thereby introducing potential conflicts of interest and necessitating the erection of so-called Chinese Walls to prevent this), and finally, guaranteed minimum commissions were removed, making things much more competitive. Wall Street went through something like this on May Day a few

years ago.

Anyway, these three changes led to the introduction of new computing systems developed in something of a rush to meet yesterday's deadline. Most important of these was the Stock Exchange Automated Quotation system (SEAQ) which several companies had to switch to by default at the last minute when they realised that their in-house systems would not be working in time. SEAQ provides information over the Topic network to 10,000 terminals about share prices - dealing is still done manually (at least until next year) although the SEAQ system is supposed to be updated continuously to reflect the trading.

There was a full-scale rehearsal last week when the Stock Exchange opened on a Saturday for the first time in its history. Not everything went smoothly and there were complaints about prices not being updated for as long as 20 minutes, making it possible to buy at one price and simultaneously sell at another. However, as late as Sunday afternoon, the chairman of the Stock Exchange Council was defiantly challenging anyone to demonstrate that this was still a problem.

Well, I'm sure that RISKS readers can guess what happened on Monday morning. The system lasted half an hour before it broke down at 8.30am! Although it was later up and running, and the problem was with the antiquated Topic network rather than the SEAQ system itself, there are fears that it could happen again under crisis. Apparently, this failure was caused by curiosity - everybody wanted to try out the new system at once, and it couldn't cope.

Curiosity is an interesting example of human behaviour causing a computer system to fail. I believe the telephone companies have a similar problem on Mother's Day when the pattern of usage is abnormal.

Another example of human behaviour has been the reaction of the dealers to the new system, to some extent invalidating the whole concept. Only time will tell whether this is just suspicion of a new technology or a real problem. However, at present the dealers are rather wary and are therefore only offering small deals on the system (up to 1000 shares) so that the big deals (100,000) are still negotiated over the telephone. This is partly a defensive move because the system is (rightly or wrongly) perceived as being slow, making it possible to offer unrealistic prices not in line with the market - the real market is off the screen. Equally, some market makers "are playing complicated games to test their competitors and this is likely to become a feature of the new markets". One dealer has even gone so far as to describe the SEAQ terminals as "useless". [This paragraph extracted from an interesting article in today's Times entitled "New screens 'fail to catch full deals'" by Richard Thomas]

Naturally, there has been a wealth of material about all this in the media recently, and today, all the papers are competing with each other for puns on Big Bang! When the dust settles on this most public of failures, RISKS archaeologists will have plenty of relics to excavate. Here is one of the more technical articles, reproduced without permission from today's Times, (28th October p.21)

Robert Stroud,

Computing Laboratory,
University of Newcastle upon Tyne.

ARPA robert%cheviot.newcastle@ucl-cs.ARPA (or cs.ucl.ac.uk if you trust domains!)
UUCP ...!ukc!cheviot!robert

++

"Big Bang shambles as computer breaks down -
Goodison blames Topic subscriber's curiosity"

by Michael Clark

Yesterday's disastrous debut for the Stock Exchange Automatic Quotations system was a prime example of Murphy's Law: "If something can go wrong, it will". But the problems encountered by dealers on the trading floor stemmed from technical problems at Topic, the Stock Exchange's own tried-and-tested screen-based information system.

Topic went off the air at 8.30am - a crucial time for traders hoping to establish the price of stocks ahead of the official start of dealings at 9am - and stayed down for more than an hour, apart from one intermission. The break also resulted in all operations on SEAQ being suspended for the same period.

Stock Exchange officials blamed a breakdown in the link between Topic and SEAQ. Market-makers feed their prices into the SEAQ computer which are then updated and displayed on the 10,000 Topic terminals situated in the City offices of brokers and fund managers.

Sir Nicholas Goodison, chairman of the Stock Exchange Council, described Topic as the world's eye on the market and said that although it had enjoyed a high level of reliability, it was six years old and considered fairly antiquated by today's standards.

A Stock Exchange spokesman quickly blamed curiosity for the failure: "The system cannot handle all the Topic sets being used at the same time."

Topic was operating at maximum capacity yesterday, receiving 12,000 page requests a minute, or 200 per second. [SEAQ itself is designed to handle 40 transactions per second, but the maximum demand yesterday was 22 per second.] Sir Nicholas said that the system had suffered a small setback which had been put right. He said that Topic had been overwhelmed by the number of page changes which, normally, it would not have to cope with. Most of it was simply curiosity by subscribers.

"If you want to put a monkey, or a dodo in a zoo, everyone will want to look at it on the first day," he said.

But it is still possible the breakdown could happen again. SEAQ encourages dealers and fund managers to use its screens more and a sudden surge of

business may overload Topic.

The Stock Exchange's technical officers say there are only a few adjustments that can be made to Topic. One may be to introduce an automatically triggered queuing system which limits the number of subscribers using the system at any one time. But many dealers fear this could lose them business.

Meanwhile, there were still complaints from market makers about the time it took for a price change to appear on Topic after dealing. There were reports of delays up to one hour. Sir Nicholas said these would be checked but still blamed market makers' own internal systems for the delay.

Physicists on SDI and engineering..

<LIN@XX.LCS.MIT.EDU>
Mon, 27 Oct 1986 20:01 EST

> From: decvax!utzoo!henry at ucbvax.Berkeley.EDU
>
> Hmmm. If a group of aerospace and laser engineers were to express an opinion on, say, the mass of the neutrino, physicists would ridicule them. But when Nobel Laureates in Physics and Chemistry express an opinion on a problem of engineering, well, *that's* impressive.

I simply point out that the Manhattan Project was run by a bunch of physicists. The H bomb was transformed from an 80 ton clunker to a practical device by physicists. These were "mere" engineering problems too.

ABM, SDI, and Freeman Dyson

Peter Denning <pjd@riacs.edu>
Tue, 28 Oct 86 11:10:29 pst

In RISKS 3.83, Ken Dymond noted that the ABM (anti ballistic missile system) debate of the early 1970s is similar to the SDI debate of the mid 1980s, and asked for sources that might shed light on the past debate. Here's one source known to me:

Chapter 7 in Freeman Dyson's WEAPONS AND HOPE is an excellent analysis of the ABM debate. He compares that debate with the ``star wars'' debate and finds both similarities and differences. He sees a role for (nonnuclear) ABM systems in a nuclear-free world, and expresses the hope that the ABM debate will one day be reopened. In contrast, he considers ``star wars'' a technical folly, for reasons having little to do with the reliability of the software systems.

Peter Denning

Search RISKS using swish-e

Report problems with the web pages to the maintainer

Search RISKS using swish-e

THE RISKS DIGEST

Forum on Risks to the Public in Computers and Related Systems

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

Volume 4: Issue 7

Friday, 7 November 1986

Contents

Risks of RISKS

Peter G. Neumann <Neumann@CSL.SRI.COM>
Fri 7 Nov 86 22:20:56-PST

"Nothing in the foregoing to the contrary notwithstanding," foresight is a great thing. I discovered a forgotten squirrelled safety copy of an intermediate draft of RISKS-4.7 in another directory, and so am very happy to be able to provide a recreation of RISKS-4.7 after all, despite the previous message announcing what I thought was my first real panic in running RISKS.

[BBOARD MANTAINERS: PLEASE REMOVE PREVIOUS JUNK MESSAGES. PGN]

Details on the British Air Traffic Control computer outage [6 Oct 86]

<Peter G. Neumann <Neumann@CSL.SRI.COM> [SnailMail from Herb Hecht]>
Thu 6 Nov 86 21:23:32-PST

On Monday, 6 October 1986, the British air traffic control system was put into manual backup mode by the crash of an IBM 9020D system that was responsible for flight-plan data. The computer in the London ATC Centre at West Drayton (near Heathrow) crashed and was down for two hours -- with traffic at Heathrow, Gatwick, and Manchester (among others) encountering delays of up to six hours. Because this system is also used by the military air-traffic control system in West Drayton, British defenses were also affected.

Overnight, ATC computer staff ``had loaded a new version of the main program containing routine updates. Software for running air-traffic control has to be changed regularly to take account of new routes, aircraft types and operating procedures for controllers.'' (Major updates are done once a year at the London center.) ``The changeover to a "new load" is normally a tricky business.'' (One million lines of code run on a six-processor system, networked with at least 10 other systems.)

Unknown to the system programming staff, the software contained an "unexpected flaw". ``The centre was planning to connect an additional computer to the existing 9020D complex. Provision for the machine had been made in the new software. But that morning the computer was not connected to the 9020D system. Unaware of this, the program began collecting data which should have been sent to the non-existent computer. Data backed up until alarms were sounded and supervisors decided to stop the system. Staff raced to adjust the 9020D and reload the old software. Two hours later, the machine was back in action.'' Meanwhile, operation reverted to the manual flight-strip operation.

[Drawn from New Scientist, 9 October 1986, p. 13. Thanks to Herb Hecht of SoHaR]

Re: UK computer security audit

Robert Stroud <robert%kelpie.newcastle.ac.uk@Cs.Ucl.AC.UK>
Fri, 7 Nov 86 13:05:21 gmt

There was an item in [the 6 Nov 1986] Guardian about the same report that my [earlier] submission described, so I can give you a better reference. The report is called "Computer Security in Practice" and is published by the Risk Management Services division of Hogg Robinson Ltd. who are a firm of insurance brokers and presumably have an office in London.

The Guardian article paints a bleak picture of just how ill-prepared for disaster the 50 or so companies visited are. 80% are not adequately

protected against fire, 96% are not protected against flood, (the two exceptions had only installed detectors after sustaining water damage previously), 70% don't have a stand-by power supply, 97% don't have enough stand-by power to keep the user areas going as well as the hardware, etc. Only 4% had fully calculated the cost of a disaster while 6% thought they had a plan but either couldn't find it or admitted that it was hopelessly out of date.

The article concluded with the observation that if these findings were typical, most companies were doing the equivalent of walking across the North Circular* with their eyes shut. However, Hogg-Robinson thought that these results were probably not typical because at least these firms had asked for a security risk audit. What about all the others?

* For the benefit of American readers who have not driven in London, I should explain that the North Circular is a notorious inner ring-road.

[Source: Guardian 6th November, p.13]

I would be interested to know of any similar studies of American companies.

Robert Stroud, Computing Laboratory, University of Newcastle upon Tyne.
UUCP ...!ukc!cheviot!robert

[By the way, the Newcastle mailer apparently ran amok sending this message -- among others. I received 20 COPIES. I probably would have received more had not John Rushby been having the same experience with a message from Tom Anderson at Newcastle. He finally made a call to Tom, who evidently initiated a rectification of the problem. I wonder whether the presence of two simultaneous messages from Newcastle to CSL.SRI had anything to do with the infinite loop! PGN]

USS Liberty (RISKS-4.1)

Matthew P Wiener <weemba@brahms.berkeley.edu>
Fri, 7 Nov 86 01:17:57 PST

REVISED SUMMARY ITEM FOR RISKS-4.1:
$!! USS Liberty: 34 dead; injured; 3 warnings to withdraw lost? (SEN 11 5)

There was a story, I believe in the Atlantic two years ago, giving some sort of "official" Israeli explanation (as told by two highly respected Israeli reporters) of how the Israelis came to "accidently" attack the USS Liberty, involving sad coincidence after coincidence on their side, with things like the properly identified US ship on the war map had its flag put aside temporarily by General X, and then General Y took his place at that point, and other such things. While their version is almost certainly a complete crock, it is intriguing that breakdowns in protocol are so freely invoked as cover stories.

(Is this a new brand of computer/systems meta-risk? That is, have we become so inured to "computer error" that we will take such as an excuse blindly?

Note that I am not referring to using the computer as a scapegoat to avoid blaming humans, just because there happened to be a computer in the pipeline. I wonder whether making a computer the catchall wholecloth scapegoat on the principle that no one would check for the real story has become SOP?)

In the long long run, by the way, the USS Liberty and the USS Pueblo incident led to the scrapping of NSA's spy ship program, with unknowable consequences. Presumably the development of spy satellites and the like filled the gap, but again, who really knows. Trying to measure the risks associated with intelligence can be well nigh impossible.

Actually, breakdowns in protocol are common in diplomacy. There was a flap some years ago about an anti-Israel vote by the US in the UN that was blamed on such. Cryptographic failure could have been responsible, but that would never be admitted.

Speaking of which, successful cryptanalysis can lead to striking diplomatic victories in sensitive treaties. Of course, the military impact of cryptanalysis is potentially unlimited.

These particular incidents do not really involve computers per se, although the mentality is identical.

ucbvax!brahms!weemba Matthew P Wiener/UCB Math Dept/Berkeley CA 94720

[The above contribution was excerpted from two informal private communications (with permission). It was not originally intended as a RISKS message. PGN]

Grassroots sneak attack on NSA

Matthew P Wiener <weemba@brahms.berkeley.edu>
Fri, 7 Nov 86 04:34:58 PST

This past week, a rather bizarre attempt to annoy NSA via computer has begun on USENET. Several people have started inserting cute words like "crypt" or "terror" or "CIA" in their signatures in an attempt to overload NSA's automatic grep for cute words in overseas traffic. Considering the minuteness of the added load, and the likelihood that NSA already filters out obvious traffic like the net, the effort is nothing more than a good old fashioned American form of protest. Even though it is using (a trivial amount of) OPM to pay for a symbolic sabotage, I love it.

But obviously uglier scenarios can be imagined. Is a grep-bomb possible?

ucbvax!brahms!weemba Matthew P Wiener/UCB Math Dept/Berkeley CA 94720

Arno Diehl <DIEHL%v750%germany.csnet@RELAY.CS.NET>

security%red.rutgers.edu%germany.csnet@RELAY.CS.NET
Subject: A variation of the Stanford breakin method

We just installed some SUN workstations (UNIX 4.2bsd) connected to
an ethernet using TCP/IP protocols.

We learned from the stanford breakin to be extremely careful when using
".rhosts". So we only entered such workstations into ".rhosts" located
in the office of trusted users.

One night a student operating a SINIX workstation experimented with
TCP/IP. He configured his machine to use the IP address of a trusted
host and he entered the username of a trusted user into "/etc/passwd"
of his maschine. Then he rlogin'ed into a SUN-workstation as a trusted user.

==> Do not use ".rhosts" unless you have EVERY host and EVERY communication
path totally under control!

Arno Diehl, University of Karlsruhe, West Germany

Re: Subject: Computers and Medical Charts (RISKS 4.5)

Roy Smith <allegra!phri!roy@seismo.CSS.GOV>
Thu, 6 Nov 86 11:54:44 est

> From: Christopher C. Stacy <CSTACY@JASPER.Palladian.COM>
> Subject: Computers and Medical Charts
>
> So, the opinion of one medical records administrator seems to concur with
> that of Dr. Tessler; the people at that hospital probably were over-reacting
> inappropriately. [...] this situation presents the familiar risk of
> paranoid confusion.

In my (limited) experience, the other problem is more common;
people under-reacting inappropriately to the security risks of storing data
in computers. We are a biological research lab and use our computer
systems to store everything from mundane experimental results to patent
applications. Somehow, people have gotten the impression that once it's in
the computer, it's safe. It's hard enough to convince everybody to keep
their password secret, let alone read-protect their files or (God forbid!)
think about encryption or off-line storage when appropriate. Even when we
had a rather sophisticated breakin a couple of months ago, and I sent
around what I intended to be a scare-the-blank-out-of-them memo, people
still trust the machine to safeguard their data more than is probably
prudent.

It gets worse. There was recently an (apparently unrelated)
incident involving researchers at two nearby research institutes where one
researcher (call him thief) stole some important data from a competitor
(victim). I got the original story from a mutual competitor of those two
who works here (fool). When I spoke with victim to get the whole story, he
admitted it was purely his fault. Victim was 1) using the same system as

thief to store his data and 2) didn't read-protect his files because he wanted certain other people to be able to read them (not thief or fool, however). I then went back to fool and told him what had happened and urged him to take at least some simple precautions -- change his password for example. He refused, saying that 1) he thought his data was safe enough and 2) he couldn't imagine that anybody would/could break in. Even when I reminded fool that he had just had a big fight with one of his post-docs and ended up firing the post-doc, he wouldn't believe me that there might be people out there with the motive and capability to steal or destroy his data!

So, what am I supposed to do? Here we have a person who, in the face of overwhelming evidence that his data might be in peril, insists on clinging to his belief that if it's in the computer, it must be safe. In my opinion, this is a far more dangerous situation than what CSTACY@JASPER reports.

DDN Net breakdown (?) on 6 Nov 86?

Will Martin -- AMXAL-RI <wmartin@ALMSA-1.ARPA>
Fri, 7 Nov 86 12:20:38 CST

Since the well-known ARPANET breakdown is one of the RISKS archive items, I was wondering if anyone on the list could contribute information about what seemed to have been a DDN (or maybe just MILNET?) breakdown that happened yesterday, 6 Nov 86? All I know of it was that our data communications people got a call from Army Communications to let them know that the reason we were off the net was not just a local area or in-house problem, but some sort of general malaise or trouble all over the network. I know no more details as to the nature or true extent of the problem(s) and would like to read details or at least a description of the symptoms. It was cleared up within hours, so was not as severe as the historic ARPANET collapse, but it would probably be worthy of mention in RISKS.

Will Martin

[I asked Ole Jorgen Jacobsen <OLE@SRI-NIC.ARPA> of the Network Information Center whether he had heard anything. ``The only thing that comes to mind is the TAC problems we had yesterday, where lots of TACs gave "bad login" and needed to be reloaded.'' PGN]

Re: Linguistic decay (RISKS-4.4)

Matthew P Wiener <weemba@brahms.berkeley.edu>
Fri, 7 Nov 86 01:26:38 PST

There was a discussion in mod.comp-soc when it was still a mailing list last spring on word processors => linguistic decay. As someone who loves the language for the sake of language, it is depressing to contemplate.

ucbvax!brahms!weemba Matthew P Wiener/UCB Math Dept/Berkeley CA 94720

Mechanical Aids to Writing

<Boebert@HI-MULTICS.ARPA>
Fri, 7 Nov 86 19:25 CST

I couldn't resist, after reading M. Minow's quoting of the redoubtable Burgess.

> Headline: "Reporters Should Cultivate the Use of the Fountain Pen"
>
> "In a recent address delivered at Columbia University, Mr. Edward W. Townsend, newspaper and magazine writer and Congressman, expressed the opinion that it was a misfortune that the typewriter had come to be so generally used in newspaper rooms, because it made the translation of thought into copy somewhat too easy. The view point is that the somewhat slower and more careful handwriting of any article or news item is better, clearer thought and is always better constructed when written with a fountain pen than when rambled off on a typewriter..."

This from the "Pen Prophet", the house organ of the Waterman pen company, Volume XII, No. 1, June 1914. So there, Red Smith, Ernie Pyle, and E. B. White.

> [A well-known exponent of pens is Edsger W. Dijkstra, much of whose EWD series is still written very carefully in pen. PGN]

Search RISKS using swish-e

THE RISKS DIGEST

Forum on Risks to the Public in Computers and Related Systems

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

Volume 4: Issue 8

Sunday, 9 November 1986

Contents

Re: Computer causes chaos in Brazilian Election

<rutgers!meccts!mecc!sewilco@seismo.CSS.GOV>
Sun, 9 Nov 86 01:14:36 EST

This situation involving computers is severe due to Brazil's laws, with which most of the RISKS readers are undoubtedly not familiar.

The "frayed tempers" due to not getting the "essential voting card" in Brazil are not simply because everyone likes to vote. Everyone MUST vote in Brazil. Proof of recent voting is one of the required legal documents for several situations, including simply getting a job. Those missing voting registration cards are the prerequisite to being able to vote and be a law-abiding citizen qualified to live a normal life. (My wife is from Brazil and had to carry those documents.)

> Programmers overlooked that twins are born on the same day to the same

> parents. Consequently, the voting rights of an estimated 70,000 twins
> were cancelled. The Federal Electoral Tribunal in Brasilia is currently
> wading through 140,000 appeals, including the case of a certain Jose
> Francisco, who says all his 14 brothers were baptised with identical
> names.

All this is familiar to analysts and programmers. The voting documents were formerly handled by humans who modified the processing procedure as required by common sense and local situations ("Yeah, I know Jose Francisco. All 14 were here last year, I still have to see 6 of them this year.") The written procedures are undoubtedly what guided the programmers. If the implementation schedule was the same for the whole country, it is little wonder that many exceptions were found at the same time.

Scot E. Wilcoxon Minn Ed Comp Corp {quest,dayton,meccts}!mecc!sewilco

---

Grassroots sneak attack on NSA

<LIN@XX.LCS.MIT.EDU>
Sat, 8 Nov 1986 09:42 EST

> From: weemba at brahms.berkeley.edu (Matthew P Wiener)
>
> Several people have started inserting cute words like "crypt" or "terror" or "CIA" in their signatures in an attempt to overload NSA's automatic grep for cute words in overseas traffic. Considering the minuteness of the added load, and the likelihood that NSA already filters out obvious traffic like the net...

That would be inconsistent with the oft-repeated claims that NSA monitors ALL overseas telephone calls. I have been told (someone pls confirm or deny?) that voice recognition technology is good enough that given Crays on an NSA budget, such a feat is possible when you are looking for certain key words, and that recognition can be done on a very limited vocabulary independent of speaker.

Comments?

Re: Grassroots sneak attack on NSA

Matthew P Wiener <weemba@brahms.berkeley.edu>
Sat, 8 Nov 86 14:33:51 PST

> Considering ... the likelihood that NSA already
> filters out obvious traffic like the net... [MPW]
>
>That would be inconsistent with the oft-repeated claims that NSA
>monitors ALL overseas telephone calls. [HL]

Of course they intercept the net, but if you were snooping around through all overseas telephone calls, you too would set some priorities.

>[voice recognition rumor]

Well if that's how they do it, I *hope* they know enough to filter the net!

ucbvax!brahms!weemba Matthew P Wiener/UCB Math Dept/Berkeley CA 94720

Ethernet Security Risks

Phil Ngai <lll-crg!amdcad!phil@seismo.CSS.GOV>
Sat, 8 Nov 86 12:49:41 pst

Security on an Ethernet is a very tricky business. If you use the Berkeley rhosts scheme, it is easy to spoof someone else's ip address, although there is some code in Berkeley Unix that detects when someone is impersonating you, the message only comes out on the system console. And if the bad guy makes your machine crash while you are away, no one will be the wiser.

If you ban rhosts and only allow ftp and telnet, you are vulnerable to people grabbing packets off the Ethernet and getting your password.

Which is worse? Would you rather freeze to death or burn to death? I don't know if it matters. I think that if security matters, it would be best not to let machines you don't trust on your Ethernet.

Sun proposed an interesting scheme at the last Usenix. Two machines that wanted to communicate would use an encrypted timestamp on each packet as authentication. This assumes, of course, that the two machines have synchronized their clocks and that they have a common key no one else knows. (their scheme included a key distribution method which I will not discuss here) There is also a performance penalty. They did some back of the envelope calculations showing it would be acceptable in many cases.

Is it unreasonable to put machines you don't trust on another Ethernet, with a router between your group and them?

Phil Ngai

Perfection

<LIN@XX.LCS.MIT.EDU>
Tue, 28 Oct 1986 10:48 EST

From: Douglas Humphrey

Information replacing knowledge

Daniel G. Rabe <<DAN09697%NUACC.BITNET@WISCVM.WISC.EDU<>
Sat, 8 Nov 86 14:20 CST

In RISKS 4.4, Martin Minow makes the point that computerization makes

it easier to substitute quantity for quality in our writing. I would go one step farther and say that the easy access to information made possible by computer systems has also degraded our ability (or at least our desire) to gain and retain knowledge.

The following is excerpted from an essay entitled "Look it up! Check it out!" by Jacques Barzun in the Autumn 1986 *American Scholar.*

``... the age of ready reference is one in which knowledge inevitably declines into information. The master of so much packaged stuff needs to grasp context or meaning much less than his forebears: he can always look it up. His live memory is otherwise engaged anyway, full of the arbitrary names, initials, and code numbers essential to carrying on daily life. He can be vague about the rest: he can always check it out.

``... But what we are experiencing is not the knowledge explosion so often boasted of; it is a torrent of information, made possible by first reducing the known to compact form and then bulking it up again -- adding water. That is why the product so often tastes like dried soup.''

As computer scientists, I think we find it all too easy to divide and compartmentalize information as we see fit. As I see it, one of the greatest risks of widespread computing is that we'll all stop learning. We've got spelling checkers, so why bother learning to spell? We've got calculators and home computers, so why bother learning any math? We've got electronic mail and conferencing, so why bother to learn or practice the art of public speaking? Are we reaching the point where being an expert simply means having a large computer database, as opposed to years of learning and knowledge? I don't think we're there yet, but I fear that our society's heavy emphasis on "information" and computing might be leading us there.

Daniel G. Rabe
Northwestern University

Word Processors / The Future of English

Stephen Page <munnari!uqcspe.oz!sdpage@seismo.CSS.GOV>
Sunday, 9 Nov 1986 14:07-EST

The interesting article by Anthony Burgess reproduced in RISKS-4.4 reminded me that when the first lap-top computers were introduced a few years ago, some professional writers noticed that their sentences were becoming shorter and their paragraphs chunkier, as they relied on a 40-column, 8-line display (e.g.) when composing texts. Has this really been cured by newer technology? Or is our familiar 80x25 model just as likely to have an adverse impact on writing style?

Copyrights; passwords; medical information

Matthew P Wiener <weemba@brahms.berkeley.edu>
Sat, 8 Nov 86 01:16:22 PST

> "How Fred lets the fraudsters in" (c) Newspaper Publishing PLC
^^^

Considering the frequency with which we see this half-circled c used as an ASCII replacement for the genuine circled c, it is obvious that a lot of people have let their primitive keyboards delude them into a non-copyright. ("Copyright", spelled out, takes longer than "(c)", but it has legal standing.)

> Passwords are particularly vulnerable when they remain unchanged for a long
> time. The chairman of one major company the auditors investigated had kept
> the same password for five years. It was "chairman".

This reminds me of the WWII story in Feynman's book about the hot-shot military big boss with his fancy-dancy super-safe: the combination was never changed from the factory original. "The more things change, the more they stay the same."

>Now, I am being accused of taking confidential information out of the
>hospital in the form of patient records and doctors names! All I had on the
>computer were my notes. The paranoid medical staff is afraid that having
>this information in my "COMPUTER" is dangerous, [...]
>Pretty amazing paranoia, huh? Do people really still fear computers this way?

In this situation, it strikes me as typical computer ignorance. But in general, the use of a computer as opposed to a legal pad leads to more security problems. Handwritten notes are both unmistakeable as such and are naturally limited in content. (I assume this is old hat to RISKers.)

ucbvax!brahms!weemba Matthew P Wiener/UCB Math Dept/Berkeley CA 94720

Search RISKS using swish-e

THE RISKS DIGEST

Forum on Risks to the Public in Computers and Related Systems

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

Volume 4: Issue 9

Monday, 10 November 1986

Contents

Risk of aging

Lee F. Breisacher <Breisacher.OsbuSouth@Xerox.COM>
10 Nov 86 12:26:56 PST (Monday)

From LA Times, Saturday, November 8, 1986:

G.C. Blodgett, a living legend as an outdoorsman in New England, drives a car to his favorite fishing spots from his home in West Babylon, Mass., but he almost quit this year when his insurance bill arrived. His son told the Providence Journal: "He wanted to know why the premium was three times as much as the previous year. So we called the insurance company, and after a

while, the fellow there came back laughing and explained that their computer calculated premiums for drivers up to 100 years old. After that, it started at the beginning again, so he was being charged the premium of a teen-ager."

Blodgett is 101.

Re: UK computer security audit

<hplabs!pyramid!utzoo!henry@ucbvax.Berkeley.EDU>
Sun, 9 Nov 86 08:40:40 pst

> The Guardian article paints a bleak picture of just how ill-prepared for
> disaster the 50 or so companies visited are. 80% are not adequately
> protected against fire, 96% are not protected against flood, (the two
> exceptions had only installed detectors after sustaining water damage
> previously), 70% don't have a stand-by power supply, ...

It is worth noting that even the companies which theoretically *are* prepared may find their preparations wasted in practice. The first NYC blackout caught a number of hospitals with, so to speak, their pants down. Things like emergency generators with electric starters! Another example that I remember was a place that had a fine emergency generator, started up properly and actually ran for a while. Trouble was, it was in the basement, which was below the local water table and was kept dry by pumps running continuously. You guessed it, the pumps weren't on the emergency power. The only people who had reliable power throughout the blackout were the professional paranoids: the military and the phone company.

It might be worth finding out whether there was any attempt to compile a list of such experiences from that blackout. I heard about this by chance.

(The electrically-started-generator problem was larger than it looked. Modern power plants need startup power for things like pumps and control systems. No need for emergency generators, you can always get startup power from the network. But what do you do when the *whole* network is down? A combination of luck and improvisation sufficed that time.)

Henry Spencer @ U of Toronto Zoology
{allegra,ihnp4,decvax,pyramid}!utzoo!henry

Lost files

<CS117341%YUSOL.BITNET@WISCVM.WISC.EDU>
Sun, 9 Nov 86 18:57 EST

[After a request to resend missing copies of RISKS-3.92, 4.1 and 4.2]

I believe these files were lost on the net on 3 Nov. Apparently, one of the computers on Bitnet had a severe hardware crash and lost about 1500 files... Unfortunately, I don't have any more info on this. Norman

[This happens far too often. I presume we need some research on really reliable, "guaranteed-service" protocols. On the other hand, the computational cost associated with such algorithms may be far too high for just sending net mail, and besides there is no such beast that will work correctly under all possible circumstances. PGN]

Canard!! [Looping Mailers]

"Lindsay F. Marshall" <lindsay%cheviot.newcastle.ac.uk@Cs.Ucl.AC.UK>
Mon, 10 Nov 86 09:40:12 gmt

Let me hasten to assure the RISKS list that the 20 messages reported by PGN were not generated by our mailer at Newcastle as far as we can tell. I think that the problem was much further down the line. Lindsay

[I thought about changing the SUBJECT line of this message to make it more explicit, but then I would be guilty of being a Canard Liner. However, since the implication of "canard" ("a fabricated story") is meaningful, I did not want to duck it. (An aquacktive nuisance.) Can anyone else provide a report of this happening elsewhere at the same time, on or around Friday, 7 Nov 86, 13:05:21 gmt? PGN]

Friend-foe identification

<hplabs!pyramid!utzoo!henry@ucbvax.Berkeley.EDU>
Sun, 9 Nov 86 08:41:08 pst

In the course of catching up on Flight International (the British analog to Aviation Leak), I ran across an interesting item in the 7 June 1986 issue. The UK Ministry of Defence officially admitted that a British helicopter, shot down in the Falklands War with all four aboard killed, was downed by a Sea Dart missile from a British destroyer. On 6 June 1982, HMS Cardiff reported shooting down an Argentine helicopter flying in darkness toward Port Stanley. It was actually a British Army Gazelle on a resupply flight between Darwin and Mount Pleasant. The lack of Argentine wreckage and the coincidence of timing were noticed, but a forensic investigation was unable to establish a firm connection. Forensic tests in the last year or so have pretty much settled the question. MoD apparently won't discuss how the misidentification occurred.

(This sort of thing is far more common in combat than most people think. In WW2 there was a standing joke about how antiaircraft gunners decided whether an aircraft was friendly or hostile: approaching = hostile, receding = friendly.)

Henry Spencer @ U of Toronto Zoology
{allegra,ihnp4,decvax,pyramid}!utzoo!henry

Micros in Car Engines

jed sutherland <jed%noah.arc.cdn%ubc.csnet@RELAY.CS.NET>
Mon, 10 Nov 86 09:32:27 pst

Considering the amount of duties undertaken by micros in today's automobiles, I can only conclude that it is a case of "Because we can do it". Sure, computer controlled fuel injection is very efficient and is a good idea. But my brother just bought a new BMW with all sorts of standard stuff on it. It will tell you the outside temperature, warn you when the temp is low enough that the roads are likely to be icy, etc. The radio is more complicated than the oil pressure, water temperature indications.

I am also amazed at the fact that one can buy a car with totally digital instrumentation. What possible advantage can there be to all of this?

I noted a while back that when boosting the newer car, one runs the risk of blowing any computer that may be on board due to power surges. These things cost about $1000 to replace. Most mechanics nowadays are trained to identify the faulty module and replace it without trying to find the bad component.

I think that the average driver loves all the pretty lights but doesn't usually use all his instruments anyway. For one thing, most drivers seem to be able to handle very little at one time and it is all they can do to keep the car between the lines. They don't need more distractions provided by today's auto-toys.

Jed Sutherland

Information replacing knowledge

Bard Bloom <bard@THEORY.LCS.MIT.EDU>
Sun, 9 Nov 86 17:41:55 est

> As I see it, one of the greatest risks of widespread computing is that
> we'll all stop learning...

Most of the time, people learn things because someone (often the person herself) thinks the things are useful. So, for instance, very few Americans this decade know a whole lot about the care and tending of a horse or about the growing seasons of various plants, despite the fact that these were vital facts for much of the American population a century or two ago. Mathematics (e.g., things like algebra and basic set theory) have become a lot more popular. As the environment changes, the set of things chosen as "essential knowledge" changes. We may expect to see this continue, and a good thing too. I don't *want* to know a lot about mucking out stables.

Some might argue that some things are good to learn in and of themselves. I'd agree for some areas (e.g., the arts), and disagree for others (e.g., spelling).

> Are we reaching the point where being an expert simply means having a large
> computer database, as opposed to years of learning and knowledge?

I hope not. We might be reaching the point where being an expert means having a large computer database as well as knowing the subject well. This is not particularly different in character from having a large physical library in one's area of expertise, which most experts do. Part of the point of expertise it that one can do things that aren't in one's library or database.

> I don't think we're there yet, but I fear that our society's heavy
> emphasis on "information" and computing might be leading us there.

Possibly so. I've noticed a general feeling that computer answers are more to be trusted than human ones.

Bard Bloom, MIT

Information replacing knowledge

<LIN@XX.LCS.MIT.EDU>
Sun, 9 Nov 1986 15:52 EST

> From: <DAN09697%NUACC.BITNET at WISCVM.WISC.EDU> (Daniel G. Rabe)
>
> As I see it, one of the greatest risks of widespread computing is that we'll all stop learning. We've got spelling checkers, so why bother learning to spell?...

It's an old fear. It was said about Xeroxing -- and who has not had the experience of copying an article in the hopes that its information would seep from the file cabinet to the brain? It was said about books and printing -- and who has not bought a book without the same experience. It was apparently even said about writing -- and who has not wished that (s)he could speak as well as (s)he could write?

That's not to say that all these fears are unjustified. But it is not new with the advent of computers.

Information replacing knowledge

Jerome H. Saltzer <Saltzer@ATHENA.MIT.EDU>
Sun, 9 Nov 86 18:52:04 EST

> [...] some professional writers noticed that their sentences were
> becoming shorter [...], as they relied on a 40-column, 8-line display...

From what I have seen of the output of some professional writers, that is a RISK that I am willing to tolerate, perhaps even encourage.

Jerry

[It even sounds like a fine idea for RISKS contributors. PGN]

Spelling becoming obsolete?

<TMPLee@DOCKMASTER.ARPA>
Mon, 10 Nov 86 00:11 EST

Yes, spelling checkers are allowing students to get by without learning to spell -- *and the schools are endorsing that trend*! I have yet (slight hyperbole here) to get over the words I heard three years ago from our oldest son's seventh-grade English teacher (yes, "English"). It was during the beginning-of-the-year parents' orientation meeting where we have the opportunity to meet all the teachers and hear their plans for the year. I can't remember the precise context any more, but I think we had asked some kind of question about whether she took spelling into consideration in grading compositions. The answer was roughly this: "Not very much -- after all, all these kids will be using word processors in the future and won't have to know how to spell." Fortunately this view was not shared by most of the rest of the teachers. (The school district, by the way, and the particular junior high itself, is among the top few percent in the country, as judged by scores on the SAT and the various awards it has received.)

They almost got me! [A motor-vehicle database saga]

<SYSMSH%ULKYVX.BITNET@WISCVM.WISC.EDU>
Sun, 9 Nov 86 15:57 EDT

I scored big on some DEC call options recently. I used the proceeds to purchase an expensive 87 turbo mazda RX-7. After driving it for a month I realized my driver's license had been expired for a year. Kentucky sends you a post card when it is time to renew. I simply assumed that mine got lost somehow and went downtown to renew. They took my license and told me it was suspended in February of 85! Arg! Since my license was suspended I did not get a renewal notice.

The clerk was very helpful and gave me a phone number to call. I called the number and the gentleman on the other end told me that because my license was issued under an older system, it would be awhile before he could retrieve my record and tell me why the suspension occurred. The State was switching over to a social security number based system, and evidently the old system existed only in hard copy form. He then said, "By the way, may I have your social security number? Please call us back after lunch and we should have some information for you."

I called back and found out that a speeding ticket obtained in February of 85 had pushed me to the limit of "points" and that the state had sent me a notice to appear at court to plead my case. If I had shown up, the judge would have given me "traffic school" and I would have kept my license. I never received any notice. I didn't show up in court so they suspended my license for 6 months in retaliation. I asked the clerk on the phone to tell me where they sent the notice. He said "6103 glimmer way apartment 4". After finding out what the procedure for getting my license back was I thanked the clerk for his assistance.

(Plot thickens here) In 1981 I lived at 8103 glimmer way apartment 4. In 1982 I moved from there, and sent the state a letter informing them of my change in address. I did not include my social security number. Since the state was converting from an older system to the new SSN based system the address change did not get made. Evidently, they just re-entered all the data from the old system to the new system and mis-keyed my address. State law states that my obligation was to inform them of a change in address.

So, bottom line, I was driving from March 85 to November 86 with a suspended driver's license. I continued to pay auto insurance. I rented cars during several business trips (I consult on the side). I get another(!) speeding ticket on the interstate. The officer called in to "run" my license, but since it was "old-system" they didn't give him the info that I was suspended. I drove off, paid the fine, never heard anything. My car was towed twice for being parked improperly, I paid the fines, showed my license, got the car back twice.

Here is the real kicker. My insurance company states clearly that they are not liable if I have an accident without a valid driver's license. The loan on the unfunded portion of my sleek black RX-7 states that if I don't maintain insurance I can be sued for the loan. What if....I had gotten in my RX-7 and wiped out some people and the car? I'd have been found to be in violation of the law, been denied insurance coverage, lost the funds I put in to the car, and still been liable for the remaining portion of the loan I took out!!!!

Well I have my license back now, smiling in my RX-7 (insured). I feel VERY lucky that nothing happened to me. The total cost for me to get out of this one was $38! It makes me wonder if there others are in the same boat (massive personal liability indirectly induced by a change from one computer record system to another). I just fell through the cracks and didn't even know it.

Mark Hittinger/systems programmer iv/ocis south center
University of Louisville, Louisville, Ky 40292
sysmsh%ulkyvx.bitnet@wiscvm.wisc.edu

Search RISKS using swish-e

THE RISKS DIGEST

Forum on Risks to the Public in Computers and Related Systems

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

Volume 4: Issue 10

Wednesday, 12 November 1986

Contents

Extreme computer risks in British business

"Lindsay F. Marshall" <lindsay%cheviot.newcastle.ac.uk@Cs.Ucl.AC.UK>
Tue, 11 Nov 86 09:54:27 gmt

FIRMS 'SUICIDAL' ON COMPUTERS, by Peter Large (From The Guardian 10/11/86)
[10 Nov 86?]

British business suffers nearly 30 computer disasters a year, involving firms in direct losses running into millions, according to a survey published today.

Datasolve, the computer software arm of Thorn EMI, questioned the UK's biggest 500 accountancy firms and found that 28 per cent of them had encountered computer disasters among their clients in the past five

years; and at least 67 per cent of those breakdowns were avoidable.

These are not cases of computer fraud or interference by young computer "hackers": they are cases of accidental loss of data, through system breakdowns or operator errors, and through fire and flood. In some cases firms have lost all records of staff pay, orders, and contracts.

Mr. Chris Wood, chief executive of Datasolve, said: "The survey shows that many firms are risking commercial suicide. Figures from the US indicate that 90 per cent of firms suffering a major computer disaster subsequently went out of business within 18 months.

"The only reason we are not seeing the same statistics here is because UK firms are currently less computerised than their US counterparts."

The Datasolve report says that small and medium-sized firms, operating micro- and mini-computers without full-time professional staff, are most at risk. The accountants questioned blamed ignorance, lack of resources, and perceived cost for the unnecessary risks that firms are taking.

Most of the accountants said that firms needed to spend between 1 and 4 per cent of their annual computer budgets on stand-by computers and other protection methods. A third of them suggested that auditors should warn shareholders if a company's protection measures are inadequate.

Alabama election snafu caused by programmer

Peter G. Neumann <Neumann@CSL.SRI.COM>
Wed 12 Nov 86 12:55:00-PST

Election results in Mobile, Alabama, were delayed for several hours due to "computer problems". According to a report on WKRG-TV in Mobile, the problem was caused by a programmer improperly opening an output file, causing the vote totals to be sent to the bit bucket. The results were not lost, they just could not be printed out until the bug was found and fixed. The delay in reporting caused the outcome of the Senate race to be undetermined for quite some time. (Mobile is the hometown of Sen. Denton, who was narrowly re-elected.) [I hope this is a correct version. I had several earlier fragmentary versions...]

> [If you suspect any hanky-panky, be sure to (re)read the previous messages on RISKS on this subject, including RISKS-2.42. PGN]

Looping mailer strikes again

Brian Reid <reid@decwrl.DEC.COM>
11 Nov 1986 2314-PST (Tuesday)

On November 7, Andrew Walker of Nottingham University sent me a mail message. I received 72 copies of the message on November 7, the first arriving at 09:53 PST and the last arriving at 17:22 PST. Two days

later on November 9 I got 21 more copies. Note that all 93 copies of this message (1890 characters) were sent across the Atlantic separately.

The guilty party is the PDP-11/44 mail relay computer at University College, London. Most outgoing mail from the UK to the ARPAnet passes through this machine. I have not contacted the management of the machine to find out what the story was.

I think that this supports Lindsay's claim that he didn't do it....
Brian

Looping mailer strikes again

Nancy Leveson <nancy@ICSD.UCI.EDU>
11 Nov 86 08:51:49 PST (Tue)

You requested any information about another similar incident. Well, on 7 Nov. 86 at 14:12:47 gmt I received 10 identical copies of a message from Tom Anderson. Nancy

---

Lost files on Bitnet (cf RISKS-4.9)

Niall Mansfield <MANSFIEL%EMBL.BITNET@WISCVM.WISC.EDU>
Tue 11 Nov 86 14:41:34 N

Losing files on Bitnet through IBM machines going down is very common. It seems RSCS holds its store and forward files in a spooling area which is often lost if the machine crashes. We get several such losses reported every month, and it's not uncommon for thousands of files to be lost.

It's hard to see why this shouldn't be fairly easy to fix:
it would certainly improve net reliability, and without any research on guaranteed-service protocols.

VOA car testing

Bill Janssen <janssen@mcc.com>
Tue, 11 Nov 86 10:19:13 CST

> [This is the tail-end of a private exchange regarding testing, e.g., for interference... PGN]

Unfortunately, that's not as singular an example as one might hope. Characterization of electrical noise under most industrial circumstances is very poor. Many microprocessor-based systems are tested with a "showering arc generator", which is a bunch of relays and coils and loops of wire hooked up to motor driven interrupters. The tester turns on the showering arc generator, places the item to be tested near it, and sees if it can perform its standard functions. This is thought to

be a "worst case" test, though in fact it's not at all clear that it is.

Bill

Re: Aftermath of the Big Bang (apology)

Robert Stroud <robert%kelpie.newcastle.ac.uk@Cs.Ucl.AC.UK>
Tue, 11 Nov 86 19:09:07 gmt

In my previous article about the Big Bang I said that one of the biggest outstanding problems was a backlog of 55,000 unmatched trade reports at the end of the first week, which had increased to 59,000 by the following Tuesday. In an attempt to put this figure into perspective, I unwisely added that "a semi-informed guess" would be that this represented about 30% of the weeks trading.

"Semi-informed" was meant to indicate that it was not totally random, but resulted from some data and some reasoning on my part. Unfortunately, both turn out to be wrong - the correct figure is 15% (I think!). My hesitation arises from having to perform two unit conversions - it said in yesterday's Independent (10th November) that "10,250 represents about 2.5% of the average number [of bargains] in a normal account". That figure is presumably correct, but there are two transactions in a bargain, and two weeks in an account, (at least, I *think* there are two weeks in an account...).

Anyway, please accept my humble apologies for dropping a factor of two due to neglecting the transactions/bargain conversion. (It was a factor of four until I remembered the weeks/account figure!)

The good news is that the number was down to 20,500 by Saturday morning and should be cleared by Thursday morning - the deadline being Friday night. I don't think it could have been 59,000 last Tuesday in that case, so maybe the problem has been not just keeping records of transactions but keeping records of the records! One of the difficulties in sorting things out has been that some of the computer systems did not allow the records of transactions to be altered (presumably to prevent fraud and preserve an audit trail).

Robert Stroud, Computing Laboratory, University of Newcastle upon Tyne.
UUCP ...!ukc!cheviot!robert

Re: The Future of English (RISKS DIGEST 4.8)

<allegra!thc@ucbvax.Berkeley.EDU>
Mon, 10 Nov 86 22:36:33 PST

The word processor is leading to a decay of the English language, and now we discover that the typewriter leads to a similar decay. Who knows what evils were caused by the fountain pen and the quill? Well, you can forget all that because the problem can be traced back much farther.

A quotation from Plato:

> ``Said Thoth to the King of Egypt, `This invention, O King, will make the Egyptians wiser and will improve their memories; for it is an elixir of memory and wisdom that I have discovered,' but the king was not convinced and feared that the invention of writing would impair the memory instead of improving it and that the people would read without understanding.''

So, papyrus started this long, slow tumble into chaos. What say you we start a lobby to bring back the clay tablet?

[Note: I don't mean to belittle the arguments that warn of the dangers of word processing. Too little thought goes into much of what I read (and write). I just thought this echo from the past brought a new perspective to the discussion.

The quotation comes from p. 134 of "Understanding Computers" by Thomas Crowley (my father)]

> [... and coincidentally, my first boss at Bell Labs in 1960! PGN]

Word-processors Not a Risk

Ralph Johnson <johnson@p.cs.uiuc.edu>
Tue, 11 Nov 86 10:16:00 CST

I do not believe that word-processors damage the quality of writing. Good writing occurs only when the document is revised and reworked extensively. If we write a document first with pen and then type it, we will get at least one chance to revise it. The problem is with those who create a document at the keyboard but never read or revise it. However, even revising a document once is not enough to gain high quality. It takes many, many revisions to create a high-quality document, for which word-processors are invaluable. This applies to software as well as to English, though few programmers seem to realize it.

Ralph Johnson

"Master, how many times should I revise my documents? Up to seven times?"
"I tell you, not seven times, but seventy times seven."

Search RISKS using swish-e

THE RISKS DIGEST

Forum on Risks to the Public in Computers and Related Systems

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

Volume 4: Issue 11

Friday, 14 November 1986

Contents

Computers don't kill people, people kill people

Howard Israel <HIsrael@DOCKMASTER.ARPA>
Tue, 11 Nov 86 11:45 EST

"Child Dies of Grill's Fumes In House Without Utilities"

Employee Error Kept Power Turned Off
(Washington Post, Sunday, November 9, 1986, pg A46)

(AP) NEW BRITIAN, Conn., Nov. 8--A mistake by a utility employe deprived a house of power and a 7-year-old girl suffocated from the fumes of a charcoal grill being used to heat the residence, state investigators said. The Department of Public Utility Control said the family of Lucita Morales had requested and been granted "hardship status", which is intended to guarantee service to needy customers. Gas and electric service should have been turned on Nov. 1, the report said, but a Northeast Utilities computer operator recorded the order incorrectly, punching a "no print" button

instead of a "print". As a result, service was not restored until Nov 3., the day after the girl was found asphyxiated in an upstairs bedroom. Police said a habachi that the girl's mother, Paula Craig, was using to cook and heat the room generated carbon monoxide.

Electric service to the home in Bristol had been shut off Sept. 30, and gas was discontinued Oct. 7. Utility Spokeswoman Jane Strachan said no action would be taken against the employe, whom she declined to identify. A department spokeswoman, Toni Blood, said the incident would be reviewed to determine whether the system for tracking the hardship cases needs improving, but no action was pending against the utility.

Avila Craig, Lucita's grandmother and the owner of the two-story house, said she did not blame Northeast for the girl's death. "It's sad so many people get caught up in the bureaucracy," she said. "It's about time people in Bristol wake up and realize people are hungry." "I don't feel victimized," she added. "My daughter was just caught up in what is happening in America .... She represents all the girls that have babies and no income."

Open microphone in the sky

<ihnp4!ihuxz!parnass@ucbvax.Berkeley.EDU>
Thu, 13 Nov 86 09:29:38 PST

NBC News reported last night [Nov. 12], and CBS News reported today, that a Braniff passenger jet nearly collided with a United passenger jet over Tennessee. An air traffic controller in Atlanta witnessed the situation on his radar screen, attempted to warn the pilots, but was thwarted because the frequency was blocked by an "open microphone".

Bob Parnass, Bell Telephone Laboratories - ihnp4!ihuxz!parnass - (312)979-5414

Computerized voting in Texas - from 4-Nov-86 New York Times

<LEICHTER-JERRY@YALE.ARPA>
14 NOV 1986 12:44:15 EST

[Remailed after delay due to Yale network-table problems.]

Computer Fraud Fought in Texas
Official Orders More Security for All Counties
That Tally Ballots Electronically

By Robert Reinhold

Houston, Nov. 3 -- The Secretary of State of Texas has ordered "additional security" procedures in Tuesday's election to prevent fraud in the 40 or so counties that use computerized vote counting and reporting.

Under the directive issued by the Secretary, Myra A. McDaniel, the computer-

generated printed log of the vote tabulation must record all operator commands and the "inputs," and the log may not be turned off at any time.

The Attorney General of Texas, Jim Mattox, is investigating charges of vote fraud arising from last year's mayoral election in Dallas. No findings have yet been issued in the inquiry, for which the state has hired Arthur Anderson & Company, the accounting and consulting concern.

According to Karen Gladney, Director of Elections in the Secretary of State's office, no significant changes in local vote-counting procedures are expected because of the directive. "Basically what we've done is ask counties if they do not already have them in place, to make sure these procedures are in place," she said, adding that state inspectors will be dispatched, as usual, to a number of counties throughout the state. She said that while the Secretary was aware of the Dallas inquiry, the order was not issued as a direct result of it.

In Dallas, Bruce Sherbet, elections coordinator for Dallas County, said the county already practiced "99 percent" of the precautions. But he said there would be a few changes at local precincts, where additional signatures from election judges and clerks would be required to validate computer tapes holding vote counts. In Houston, where, unlike Dallas, ballots are tallied at a central station, officials said there would be no difference. "There is nothing in the directive that we don't do all the time," said Anita Rodeheaver, a voting official in Harris County.

In Texas counties using electronic tally systems, people vote either by punching holes in a card that is read by a machine or by marking boxes that are read by optical scanning.

Among the other security procedures ordered, computer terminals outside the central counting station are to be permitted only to make inquiries, and the county clerk or election administrator must produce at least three cumulative reports in the course of tabulation and prepare a report on the number of ballots cast in each precinct. As a final measure, the Secretary of State said she had the authority to order a manual count of the original paper ballots to verify the accuracy of electronic counts.

Problems with HNN

Alan Wexelblat <wex@mcc.com>
Thu, 13 Nov 86 09:34:23 CST

Last night, at around 6:40PM CST, the Headline News Network (HNN) signal was disrupted for about 10 minutes. The picture that replaced it was too distorted to see but the audio was fairly clear. It was an advertisement for satellite-signal de-scramblers.

Does anyone have any info on why/how this happened? Did someone deliberately spoof the HNN signal? Or was it just an accidental foulup?

Alan Wexelblat

UUCP: {seismo, harvard, gatech, pyramid, &c.}!ut-sally!im4u!milano!wex

Post-hacker-era computer crime

<Mandel@BCO-MULTICS.ARPA>
Thu, 13 Nov 86 09:09 EST

Predicting Future Trends in Computer Crime:
The Post-Hacker Era
Dr. Sandy Sherizen
President, Data Security Systems, Inc.
Wednesday, November 19, 1986, 7:30 PM at MIT (see below)

Abstract: This talk is based on a paper that examines computer crime patterns and suggests the factors which will lead to increasingly sophisticated computer crimes and criminals in the future. There are several recent aspects of computer crime which indicate that computer crime has turned a corner, dramatically changing from earlier and possibly less serious versions. As we enter what can be called the post-hacker era of computer crime, we need a social road map which will guide us in preparing information security measures and computer crime laws. The information in the paper/talk is from a series that Sherizen is preparing on criminological models of computer crime.

Dr. Sherizen, a criminologist, consults with corporations, banks, and governments on computer crime prevention. He specializes in information security, providing executives with a translation of complex technical requirements into managerially relevant policies and controls. Author of "How to Protect Your Computer" and numerous articles, he has written reports for the U.S. Congress' office of Technology Assessment and conducted seminars around the U.S. and Asia.

(Sponsored by Computer Professionals for Social Responsibility)

CPSR/Boston meets on the third Wednesday of each month, at 545 Technology Square, in the lounge on the 8th floor. 545 Tech Square is located at the corner of Main and Vassar Streets in Cambridge, near the Kendall Square stop on the red line. Meetings are free and open to the public, and free parking is available.

For more information, contact CPSR/Boston at P.O. Box 962, Cambridge, MA, 02142, or call (617) 666-2777.

They almost got me! [A motor-vehicle database saga] (Mark Hittinger)

"Maj. Doug Hardie" <Hardie@DOCKMASTER.ARPA>
Wed, 12 Nov 86 09:50 EST

I had a similar situation in college many years ago. However, the

associated risks were much different. The school had a honors program in humanities that replaced al the undergraduate general requirements with one two-year course. Competition to get in the program was stiff. As I remember the requirements, you had to have all A's in English etc., plus outstanding scores on the entrance exams. Only 1 percent or so of each new class was selected for this program. It was a real honor and a big deal was made at our hign school graduation for those who were accepted. I graduated from highschool with 2 D's in English and never expected to be considered for this program. However, the day after graduation, I received an invitation which I accepted immediately. It was a great program. However, 4 or so years later, I was running the school's computer center. The admissions people asked me to rewrite their program which selected new students for the humanities program. Since they paid real money, I took the job. The original program was written in machine language, not assembler language. It had one instruction per card in numeric form. That was a common approach in the school. Since the program was unintelligible, they provided the old algorithm and the new. It took a few hours to get the new program working. Basically, each student had a card which contained the necessary information. All that had to be done was to compare the various values on the card with the criteria and select only those that met the criteria. The admissions people provided a deck that had been run earlier so it was simple to test the new program by running it and comparing the outputs. After doing that, we found the new program selected one less person than the old. After extensive analysis, we discovered that the extra should never have been selected in the first place. That caused some consternation in the school as it meant that someone who was not qualified had taken a valuable slot in the program. So the immediate question was how many times could this have occurred? The analysis indicated that there was only one possible way to be selected improperly and it required a specific set of values for some 20 different items (including 2 D's in English). That set off a bell, and I went back to my hysterical records and found my copy of my card from years earlier. There were at least two who made it through that filter.

-- Doug

Re: information replacing knowledge

"Col. G. L. Sicherman" <colonel%buffalo.csnet@RELAY.CS.NET>
Wed, 12 Nov 86 14:16:08 EST

I sympathize with Daniel G. Rabe's argument about communication:

> As I see it, one
> of the greatest risks of widespread computing is that we'll all stop
> learning. We've got spelling checkers, so why bother learning to
> spell? We've got calculators and home computers, so why bother learning
> any math? We've got electronic mail and conferencing, so why bother
> to learn or practice the art of public speaking?

But I doubt that the millions of otherwise intelligent people who cannot spell right will agree with this characterization of learning! Indeed, all his examples belong to specific media of communication.

"Standard" spelling did not exist in Shakespeare's day; words were spelled out ad hoc. The pressure to spell each word in just one way came from printing, when people discovered that they could read faster than they could listen. Standard spelling is invaluable for the efficiency of reading print.

The flip side is that standard spelling is _not_ invaluable for electronic communication, because efficiency no longer matters--it's a measure left over from the machine age. Efficient absorption is important only in one-way, bulk media like print. Electronic communication is interactive.

Similar arguments about the nature of mathematics turn up now and then in journals like _Mathematics Magazine._ Modern mathematics is designed for the page; its methods don't allow for a Ramanujan. As for public speaking, print killed it long ago! Listen to any political debate and you'll know what I mean. Oratory is just a toy these days.

All technological progress alters us. "Why learn to walk great distances when we have trains? Why learn beautiful handwriting when we have typewriters? Why learn to use tinder and flint when we have matches?" And of course the ancient "Why learn to remember everything we hear when we have paper, ink, and alphabet?" Just remember:

1. You don't have to go along with it. Dijkstra is said to write his books with pen and ink.
   [Knuth too!]

2. If you don't like how progress alters people, you can associate with resisters like yourself--if you can find them. For example, people who believe that the prevalence of clothing weakens the body's natural defenses tend to congregate.

3. Let others choose for themselves; don't moralize about it. I for one intend to go on using spelling checkers, e-mail, and clothes.

[I rejected a bunch of other messages on this topic, as we begin to get into second-order points and some repetition. Thanks, anyway. PGN]

Search RISKS using swish-e

THE RISKS DIGEST

Forum on Risks to the Public in Computers and Related Systems

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

Volume 4: Issue 12

Sunday, 16 November 1986

Contents

Air Traffic Control radar problems

Peter G. Neumann <Neumann@CSL.SRI.COM>
Sun 16 Nov 86 20:33:49-PST

(Adapted from AP, 12 Nov 86) Radar controlling high-altitude air traffic from the Texas Panhandle to southern California was knocked out for 40 minutes by a power failure at the Albuquerque NM ATC. In addition a radar station near Phoenix, Arizona, was down for more than 59 hours due to a power failure. Both power failures occurred on 6 Nov 1986. The Albuquerque failure was the first there in 18 years, according to the FAA sector manager. The backup procedures are very awkward, but they worked well to avoid any accidents.

Stuck Microphone and Near-Collision of 727s

Peter G. Neumann <Neumann@CSL.SRI.COM>
Sun 16 Nov 86 20:40:24-PST

A stuck cockpit microphone jammed a controller-pilot frequency last week and prevented an air traffic controller from warning two Boeing 727 jetliners that they were on a collision course. The Braniff and United planes carried 175 people, and passed perpendicularly within something like 500 feet of one another. (The Sunday NY Times News of the Week in Review, 16 Nov 86, noted that there were 777 near collisions in 1985, about 30 percent of which involved scheduled airliners.)

Gwinnett County Voting

Scott Dorsey <kludge%gitpyr%gatech.csnet@RELAY.CS.NET>
Thu, 13 Nov 86 18:36:13 est

A recount of votes in Gwinnett county, Ga. has led to a few interesting problems that might be of interest to readers of Risks. Ballots from one area were accidentally not counted in the first tally, because they had been mislaid in a stockroom (and possibly tampered with). There was apparently no safeguard to prevent anyone from recognizing that a large population was not represented. Later, it was discovered that the tabulating machines used for the counting gave different results between runs. Although there is some question about the reliability of the count, it seems to be accepted as accurate.

Stan Kelly-Bootle speaks of "CREVM", the Conditioned Response Electric Voting Machine, which trains voters to press the correct lever by a series of electric shocks.

Scott Dorsey, ICS Programming Lab, Rich 110,
Georgia Institute of Technology, Box 36681, Atlanta, Georgia 30332
...!{akgua,allegra,amd,hplabs,ihnp4,seismo,ut-ngp}!gatech!gitpyr!kludge

[In nearby Alabama, the Shelby-Denton election was still unresolved according to the last report I saw (in the 12 Nov 86 Washington Post). It seemed that each recount reversed the previous one, with more new votes being discovered each time for the previous apparent loser, who became the new apparent winner. PGN]

Micros in cars

Paul Kalapathy <convex!paulk@a.cs.uiuc.edu>
Fri, 14 Nov 86 19:41:12 cst

Personal anecdote: A close friend of mine bought a 1984 Firebird. He was somewhat dissatisfied with the performance given that it had a moderately large engine. He is a software weenie, and had a friend who went to work for GM doing whatever it is they do with those micros they put in

cars to control the engine. This friend of his provided him with the commented source code for the ROMs that are in the micros for that particular model. The ROMs were of the variety that is compatible with 2716s or 2732s or one of the other common EPROMS. So, my friend proceeded to mangle the micro in his Firebird to include a socket for the EPROM. He programmed an EPROM to change the fuel mixture vs. engine speed, etc. The car had better performance, and a top speed about 30mph higher than before his modification (the gas mileage was substantailly worse, as were the noxious emissions, I suppose). In a word, it became a race car.

I don't know what risk this poses to society, but it is rather amusing.

-Paul Kalapathy

[There are some interesting warranty and liability questions as to what the manufacturer and dealer roles are once you have tinkered. There are also questions about what happens if you market such an extension, if it fails and causes loss of life, etc. PGN]

DMV computer networks

Bob Campbell <hpdsd!campbelr@hplabs.HP.COM>
Sat, 15 Nov 86 01:03:39 pst

My license also fell prey to the magic of computers. Two miles across the Ohio border, I was stopped going down a rather large hill and ticketed for speeding. Being a college student that would shortly be hundreds of miles away, I spent the money for the ticket in my local pub.

I was ticketed on my Illinois license which had the address of my father's old house. After graduation, I packed my bags and set out for California. After living here for six months, I received notice from my insurance agent that my policy was about to be cancelled. It seems that they had finally checked and found that my Illinois license had been cancelled by the state of Ohio.

The California DMV didn't care about my past record or that the license was expired. They stapled my old license to a form and in a quick (for CA) two months I had a valid license.

After paying bozo rates for 6 months with an insurance agent who worked out of his car, I decided to check around. Worried about losing coverage again, I told the whole sad story to the agent. Bad record, dropped policy and all. She called the California DMV to run a check. Three days later I was not only insured, but I now get the good driver rate.

I ran through computers that talked too much, that ignored each other and that had the right information but didn't bother to tell. Also involved were the "computers must be right" people who wouldn't let me pay the higher rates. (Not that they had to work to talk me out of it :-)

If nothing else, I think I figured out why so many bad drivers seem to be on California highways . . .

Bob Campbell Hewlett Packard Information Technology Group
hplabs!hpdsd!campbelr

Serious security bug in 3.4

Dave Martindale <dave%onfcanim.waterloo.edu@RELAY.CS.NET>
Mon, 10 Nov 86 15:10:17 est

In the 3.4 release, the cp/mv/ln command is setuid root in order to be able to rename directories. (Cp, mv, and ln are three links to the same file). Unfortunately, it isn't careful enough about where it makes use of its root privileges. Making use of this bug, anyone can become the super-user by typing just a few commands.

I do not intend to describe this method of breaking security here. However, to avoid becoming victim to it, you should remove setuid from cp/mv/ln. Although this means that only root will be able to rename directories, I can see no other way of protecting yourself from the bug until SGI fixes the program.

This bug existed in a previous release and I reported the problem to SGI. Whoever "fixed" the bug simply masked some of the symptoms without fixing the problem. I've reported it once again; let's hope they fix it correctly this time.

Dave Martindale, watmath!onfcanim!dave

"Maj. Doug Hardie" and his story

<Bruce_Schuck%SFU.Mailnet@MIT-MULTICS.ARPA>
Sat, 15 Nov 86 08:58:40 PST

I certainly hope the Major left that filter in place.

Maybe programs like the one he describes should have the occasional student who doesn't fit the profile just to see what the result is.

In this case it seems to have worked out.

Necessity of language skills

Daniel G. Rabe <<DAN09697%NUACC.BITNET@WISCVM.WISC.EDU<>
Sat, 15 Nov 86 14:58 CST

I do hope we're not beating this topic into the ground, but I am compelled to respond to Col. G. L. Sicherman's response to my orignal message on the dangers of letting computers do our thinking.

I agree with his point that

> Standard spelling is invaluable for the efficiency of reading print.

Then he says:

> The flip side is that standard spelling is _not_ invaluable for electronic
> communication, because efficiency no longer matters--it's a measure left
> over from the machine age. Efficient absorption is important only in one-
> way, bulk media like print. Electronic communication is interactive.

I cannot agree that "efficiency no longer matters". Electronic communication puts unprecedented amounts of information at our fingertips. Now that we have so much more to read, efficient absorption is even more important.

Even if the interactive nature of electronic communication makes it easier to ask for clarification or to ask questions, we must still communicate with some people non-electronically. Non-computer people often judge communication skills by one's ability to follow the standard rules of spelling, grammar, and punctuation. If we ignore these rules, we will probably just alienate ourselves from those who follow and respect them.

This introduces another potential risk: that the inability to communicate effectively with non-computer professionals will adversely affect the usability of the systems we develop for them. An even more immediate risk is a loss of confidence: "He can't even follow the rules of English; how can I be sure he's a good programmer?" From our perspective, this is an obvious _non sequitur_; from another perspective, it might make a lot of sense.

(To make myself clear, I don't consider "following the rules" to be any indication of intelligence or ability. The point is that a lot of people consider language skills to be a prerequisite for effective communication.)

[Since Daniel started this one, I thought I'd let him have another shot. But I am still rejecting most commentaries on this subject. PGN]

Call for Papers -- Safety and Reliability Society Symposium

Nancy Leveson <nancy@ICSD.UCI.EDU>
14 Nov 86 20:52:37 PST (Fri)

"Achieving Safety and Reliability with Computer Systems"
Manchester, United Kingdom, 11-12 November, 1987

Papers relating to the following system aspects of real-time computers are invited:

Integrity throughout the lifecycle
Safety Assessment
Reliability Assessment
Reliability Criteria

Safety Criteria
Specification for safety and reliability
Design for safety and reliability
Architecture for safety and reliability
Development for safety and reliability
Operation for safety and reliability

Papers are also invited that report on experience of the implementation and use of computers in safety and reliability critical applications.

HOW TO SUBMIT A PAPER

Synopses giving the title, authors, affiliations, and up to 500 words should be returned to the organiser by 7 January 1987. The initial selection of papers by the International Programme Committee will be based on the synopses. Authors will be notified of acceptance at synopsis stage by 28 February 1987. Full text papers of not more than 4000 words required before 15 May 1987. Papers will then be reviewed, and formal acceptance notified to authors in July 1987 following satisfactory revision of the paper by the author.

ORGANISER: SARSS '87, The Safety and Reliability Society Ltd., Clayton House, 59 Piccadilly, Manchester M1 2AQ, United Kingdom

INTERNATIONAL PROGRAMME COMMITTEE: B.K Daniels, Chairman; T. Anderson, UK; N. Leveson, USA; E. de Agostino, Italy; R. Bell, UK; P. Bishop, UK; R. Bloomfield, UK; S. Bologna, Italy; J. Cullyer, UK; G. Dahll, Norway; W. Ehrenberger, Germany; R. Genser, Austria; J. Gorski, Poland; G.B. Guy, UK; E. Johnson, UK; S. Lindskov Hansen, Denmark; S.R. Nunns, UK; I. Pyle, UK; W.J. Quirk, UK; J.M.A. Rata, France; F. Redmill, UK; C. Roberts, Belgium; B. Runge, Denmark; L. Sintonen, Finland; I.C. Smith, UK; U. Voges, Germany; T. Williams, USA; R. Yunker, USA

Search RISKS using swish-e

THE RISKS DIGEST

Forum on Risks to the Public in Computers and Related Systems

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

Volume 4: Issue 13

Tuesday, 18 November 1986

Contents

Framing of life-and-death situations

Jim Horning <horning@src.DEC.COM>
Tue, 18 Nov 86 17:31:40 pst

In the "1986 Accent on Research Magazine" published by Carnegie Mellon University there is an article on "The Science of Decision Making" by Robyn Dawes. The whole article is interesting, but I was particularly struck by a passage that succinctly states an issue we have often skated around in Risks:

> ... Such a contradiction violates any model of human decision making based on a premise of rational choice. Such framing effects also lead decision makers faced with life and death situations to act conservatively when the alternatives are framed in terms of lives saved (because the first life saved is the most important), but take

> risks when the same alternatives are framed in terms of lives lost (because the first life lost is the most important--thereby leading to a desire to avoid losing any lives at all). The result can be a contradictory choice for identical life and death problems, depending upon how they are framed.
>
> ... have demonstrated not only that framing affects decision, but that people systematically violate the rules of probability theory by adopting--either explicitly or implicitly--certain heuristics to evaluate the likelihood of future outcomes. ...

Jim H.

On placing the blame

Peter J. Denning <pjd@riacs.edu>
Tue, 18 Nov 86 14:34:50 pst

In recent issues of RISKS there were two items that on the surface did not appear to be in the stated purview of RISKS:

A. Two jetliners in near-miss. Controller unable to warn the pilots because there was an open microphone jamming the frequency.

B. Young girl suffocates from carbon monoxide fumes generated by home grille after power company turned off power for non-payment of bills but delayed resumption due to operator error.

I asked Peter Neumann about this. With respect to (A), he said, radar is a vital component of the system: it is called INPUT. Vulnerabilities of radars affect the ability of the computer to do its job. With respect to (B), he said, a computer operator put in incorrect data, which contributed to the problem.

In both cases, there is a total system containing an embedded computer system. In (A), for example, the total system includes the jetliners, the pilots, the radars, the radios, the computers, and the controllers. In (B), the total system includes the customers (especially the unfortunate family), power distribution, review of requests for welfare status, and the computer accounting system.

In both cases, there is a temptation to ascribe safety failures in the total system to one of its components, the embedded computer, and by implication to make the designers of that software responsible. In (A), the computer could not possibly have compensated for jammed radio frequencies. In (B), there is a possibility that, had the computer operator entered correct data, power would have been restored a few days sooner, in time to forestall the death of someone in that household; however, the child's parent, not the computer designers or operator, chose to heat the cold house with a lethal fuel and to defer application for welfare status until after the power was turned off.

In both cases, a variety of factors combined to create the unfortunate circumstance. The embedded computer systems could not have been programmed to prevent the mishap. And yet the news reports contain suggestions that computers, or their operators, are somehow at fault. Have some journalists become unduly accustomed to fingering the computer for every mishap? Have some computer people become unduly eager to accept the blame when there is a mishap in a system that contains a computer?

Peter Denning

Computer picks wife

<Matthew_Kruk%UBC.MAILNET@MIT-MULTICS.ARPA>
Mon, 17 Nov 86 08:00:52 PST

(Associated Press) November 15th

IZMIR, Turkey - A man who divorced his wife after a bitter six-year court battle and turned to a computer service to find himself the "ideal" mate was surprised when - from 2,000 prospective brides - the machine selected his former wife.

"I did not know that my ex-wife had been the ideal counterpart for a marriage," Suleyman Guresci was quoted as saying by the Anatolia News Agency before re-marrying Nesrin Caglasa.

"I decided to try being more tolerant toward her," He said.

The couple, whose first marriage lasted 21 years, were divorced nine months ago due to "severe disharmony" after living apart for six years, Anatolia reported.

Re: Micros in cars

Brint Cooper <abc@BRL.ARPA>
Mon, 17 Nov 86 15:42:40 EST

There's another risk of re-programming your engine control ROMs. It's a federal offense to remove or alter the operation of emission control equipment. Since fuel mixture and ignition affect emission levels, they are considered emission control.

Re: They almost got me!

Will Martin -- AMXAL-RI <wmartin@ALMSA-1.ARPA>
Tue, 18 Nov 86 9:50:24 CST

Your note on RISKS impressed me tremendously. What you described has so many odds against it that the fact that it happened just HAS to be significant. Just what that significance is, I am not sure, but it must be important! The odds against the occurrence of the unlikely combination of grades and data that would get through the filtering code are themselves high, but, as you said, at least two people's records produced this -- the number of possible students and their grade combinations could easily explain this, so that, in itself, isn't significant. But the fact that you, yourself one of these very few that fit this unusual mix of historical data and participated in this special course, were then asked to rewrite the computer program that contained this flaw is an incredible coincidence in itself. However, the fact that this was a special honors humanities course, the graduates of which would NOT be likely to be computer or programmer types, takes the odds out of the merely "incredible" category and puts them into some utterly indescribable astronomical range.

Thanks for sharing this with us.

Regards,
Will Martin

Joe Pistritto (JHU|mike) <@RELAY.CS.NET,@CSNET-RELAY.CSNET:jcp@BRL.ARPA>

[+ SECURITY@RUTGERS]
Subject: Re: A variation of the Stanford breakin method

What you have here is the standard 'spoofing' problem. I think the only way to control this problem (for a system attached to the Internet) is to route all the traffic thru a gateway (over which you have physical access control) that will DROP immediately any packets originating from the Internet world with SOURCE addresses that are anywhere on your local nets. (You could put insecure nets on the other side of a similar gateway inhouse, to protect the 'trusted' networks.) Prevents anyone from spoofing along as one of your hosts. (This might cause some loopback features of TCP to stop working in some implementations, however) And yes, it means that the 'trusted' hosts have to be on 'trusted' networks that are physically distinct (and of course physically secure).

Begins to sound like DoD already, doesn't it...
-jcp-

PS: Security is a pain the ass... [So may be the absence of security! PGN]

Microfiched income-tax records stolen

John Coughlin <JC%CARLETON.BITNET@WISCVM.WISC.EDU>
17 Nov 86 23:41:00 EST

It was announced in the Canadian House of Commons today that microfiche

containing personal income tax records for 16 million Canadian taxpayers was stolen from a Toronto office of Revenue Canada on November 4. The microfiche was returned November 17 after being retrieved by the RCMP. It is not known whether the material was duplicated by the thief, who has not been identified.

CTV news said that several hundred people had access to the microfiche in the Toronto office. Duplicate copies are kept in several district offices as well. This incident adds a new dimension to the recently discussed RISKS of easily portable information media, such as hospital medical records on computer diskettes.

/jc

[This item is at first blush of marginal relevance to RISKS strictly from the computer point of view -- unless the microfiche was computer generated (it was probably just a record of actual returns). Nevertheless, I include it as symptomatic of the deeper problems. PGN]

Re: Copyrights (RISKS DIGEST 4.8)

Andrew Klossner <tektronix!hammer.TEK.COM!andrew@ucbvax.Berkeley.EDU>
Mon, 17 Nov 86 10:23:58 PST

[Andrew wished to clarify the issue of whether there is a risk in using "(c)" or a half-circled "c". Although his response does not seem strictly RISKS related, I think it may clarify a thorny issue for some of you who are willing to contribute to RISKS but want to protect your rights. I have abridged it somewhat. PGN]

It is the considered opinion of the chief legal counsel at Tektronix that the genuine circled-c can be replaced only by the string "Copyright (c)". Both the word "Copyright" and the pseudo-glyph "(c)" are required...

The three basic elements needed to obtain copyright protection in the United States and the member countries of the Universal Copyright Convention (most countries of any significance) are the copyright symbol (circle-c or string "Copyright (c)"), the name of the copyright owner, and the year date of first public distribution. The law requires that the notice "be affixed to the copies in such manner and location as to give reasonable notice of the claim of copyright."

The phrase "All rights reserved" extends protection to member countries of the Buenos Aires Convention who are not also members of the Universal Copyright Convention (a few Latin American countries).

Whenever the program or document is revised significantly, the year date of the revision must be added to the notice, as in:

Copyright (c) 19XX, 19YY.

When licensing software to the (US) federal government under the the Defense Federal Acquisition Regulation Supplement (DFARS), a completely

different set of legends is required.

-=- Andrew Klossner (decvax!tektronix!tekecs!andrew) [UUCP]
(tekecs!andrew.tektronix@csnet-relay) [ARPA]

Search RISKS using swish-e

THE RISKS DIGEST

Forum on Risks to the Public in Computers and Related Systems

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

Volume 4: Issue 14

Wednesday, 19 November 1986

Contents

Re: On placing the blame (RISKS 4.13)

Matt Bishop <mab@riacs.edu>
Wed, 19 Nov 86 15:59:31

There's an old joke about computer scientists who build the most advanced, intelligent computer ever. As a test, they ask it "Is there a God?" It responds, "There is now!"

Sadly, a lot of people tend to think of computers as infallible. (We've discussed this in Risks before, I think.) Computer scientists know better, and try to educate the public to this fact of life. Peter Denning asks "Have some computer people become unduly eager to accept the blame when there is a mishap in a system that contains a computer?" If the answer is yes, one cause may be an eagerness to demonstrate to the public that the machines are not perfect.

Others once thought of the computer as infallible but have come to realize it is only as good as the people who build it, program it, and feed it data. When something (or someone, for that matter) once put on a pedestal falls off, there is a very human tendency to be more harsh towards that thing than something never put on a pedestal. We may be seeing some of this in "journalists [becoming] unduly accustomed to fingering the computer for every mishap" (although I suspect it's not just journalists who do this!)

There's also a third tendency at work here -- it's a lot easier to blame

someone whom you don't have to look in the eye. With a human, you would have to (say, when you were firing him, when you were prosecuting him, or so forth.) Also, a human can strike back verbally or nonverbally. A computer can do none of these things, and best of all you don't have to think about its feelings when you chastise it. Maybe that's part of it too.

Matt Bishop

At last, a way to reduce [net]news traffic

Matthew P Wiener <weemba@brahms.Berkeley.EDU>
Wed, 12 Nov 86 14:41:03 PST

Newsgroups: net.news
From: jerry@oliveb.UUCP <Jerry Aguirre, Olivetti ATC; Cupertino, Ca >
Date: 11 Nov 86 17:39:44 GMT

Most of you are probably aware that there was a premature posting of newsgroup messages for all the proposed newsgroup renamings. This caused many (if not most) sites to exceed the maximum allowed number of newsgroups in their active files. Some sites are still recovering from this problem.

It is interesting to note that the volume of news articles for last week was less than half what it was for the previous week.

Oct 27 11:48 to Nov 1 23:58 6,755 articles
Nov 1 23:59 to Nov 10 15:15 3,102 articles

The reduction in volume gives you some idea of the number of sites that were blown off the air.

I know it took me a couple of hours to clean up old newsgroups, recompile news with larger tables, and reprocess the failing batches. (My news daemon renames and saves batches when rnews exits with an error status.) Multiply that times the number of sites on the net and you probably get many thousands of manhours spent cleaning up.

Amazing to think how vulnerable the net is to the actions of one individual.

Jerry Aguirre, Olivetti ATC

[And this was precisely the glitch that triggered the macro error that led to the saga prior to the real RISKS-4.7! To add to the irony, MPW's message slipped through a crack last week while I was travelling. I just found it while cleaning up the RISKS mailbox! PGN]

Safety-Critical Software in the UK

Peter G. Neumann <Neumann@CSL.SRI.COM>
Wed 19 Nov 86 14:20:48-PST

[John Rushby called to my attention a remarkable report on the British view of software in the future. The entire report is fascinating reading, but in particular the following appendix is of sufficient interest to the RISKS community that it is reproduced here in its entirety for the private use of RISKS readers. It represents an important step toward the problems of developing safety-critical software. PGN]

``Software: A Vital Key to UK Competitiveness''
Cabinet Office: Advisory Council for Applied Research and Development (ACARD)
London, Her Majesty's Stationery Office. (C) Crown Copyright 1986

Appendix B: Safety-Critical Software

The problem: non-technical

B.1 No computer software failure has killed or injured a large number of people. It is just conceivable that such a tragedy could occur. What steps should be taken to:

* prevent such a disaster,

* cope with it when it does occur,

* ensure such a disaster, having happened once, cannot recur?

The problem: technical

B.2 Stored-program digital computers must be among the most reliable mechanisms ever built by man. Millions of computers throughout the world are executing millions of instructions per second for millions of seconds without a single error in any of the millions of bits from which each computer is made. In spite of this, nobody trusts a computer; and this lack of faith is amply justified.

B.3 The fault lies not so much in the computer hardware as in the programs which control them, programs full of the errors, oversights, inadequacies and misunderstandings of the programmers who compose them. There are some large and widely used programs in which hundreds of new errors are discovered each month; and even when these errors are corrected, the error rate remains constant over several decades. Indeed it is suspected that each correction introduces on average more than one new error. Other estimates offer the dubious comfort that only a negligible proportion of all the errors in these programs will ever be discovered.

B.4 New computers are beginning to be used in increasingly life-critical applications, where the correction of errors on discovery is not an acceptable option, for example industrial process control, nuclear reactors, weapon systems, station-keeping of ships close to oil rigs, aero engines and railway signalling . The engineers in charge of these projects are naturally worried about the correctness of the programs performing these tasks, and they have suggested a number of expedients for tackling the

problem. Many of these methods are of limited effectiveness because they are based on false analogies rather than on a true appreciation of the nature of computer programs and the activity of programming.

B.5 The steps which ACARD has been considering in answer to the introductory question are discussed under the following headings:

* Disaster prevention

* Disaster management

* Disaster analysis

Disaster prevention

B.6 The initiative for disaster prevention must come from the UK government and system customers. Current software is built, operated and maintained using methods and tools which are not keeping pace with the development of the hardware, nor with the increased sophistication demanded by new applications; nor does it take account of progress of research into the reliability of programs. The necessary improvements in software engineering require investment in advanced development and production techniques, education, training and legislation. Legal obligations should be at least as stringent as those imposed by the Data Protection Act, and the care and time required for detailed drafting of legislation will be just as great. A start must be made immediately.

B.7 The remainder of this appendix outlines an imaginable solution that may emerge over the next fifteen years. It is intended to promote rather than to pre-preempt a discussion of the details.

Registration

B.8 A register must be established of those (software) systems which, if they fail, will endanger lives or public safety.

Operation (demand side)

B.9 Before any organization can operate a life-critical computer system it must first obtain a License To Operate (LTO), which will only be issued when the operator can demonstrate that certain conditions (detailed below) have been met.

B.10 Each life-critical system must be operated by a Certified Software Engineer who is named as being personally responsible for the system. This Certified Software Engineer must have received the appropriate mathematical training in safety-critical software engineering.

B.11 A life-critical system must be adequately maintained; this must be one of the conditions of the LTO. Maintenance (that is, rectification and development) must be the responsibility of a named

Certified Software Engineer.

Certification

B.13 An LTO must only be granted when a Safety Certificate has been issued. Certificates must be issued for limited periods, for example, five years. Operational systems will thus need to be recertificated (relicensed) periodically (analogous to Certificate of Airworthiness).

Reliability data collection

B.14 To aid research into system reliability, and to assist Boards of Enquiry, all registered life-critical software systems must supply operating data on the Licensing Authority.

Disaster management

B.15 In the past, the danger arising from failure of computer hardware and software has been limited by switching off the computer and reverting to manual operation if necessary. In future, there will be applications for which this fall-back procedure is not available. The computers will have to continue to run, and any necessary software changes and corrections will have to be inserted into the incorrectly running system. For these applications, specially stringent precautions are necessary.

Procedures

B.16 The Licensing Authority should require disaster management procedures to be laid down in advance of operation and practiced regularly during operation (that is 'fire drill practice'). The documentation of the system must need a standard which would permit a team of experts/specialists to master it during the progress of an emergency.

Data Logging

B.17 The disaster management procedures should include the logging of data so that any subsequent Enquiry can ascertain the progress and cause of the disaster (analogous to the 'black box recorder' in an aeroplane).

Emergency call-out

B.18 There must be more than one Certified Software Engineer available to the operating company; and a duty rota should ensure that one of them is always available at short notice. Procedures must be set up for calling out a team of expert specialists in a longer-lasting emergency.

Disaster analysis

B.19 During the normal (safe) operation of any life-critical system, data on its performance and reliability must be made available to the Licensing Authority. This data will be made available to any Enquiry. (This is additional to the data logging required in para B.14.)

Board of Enquiry

B.20 Any disaster should be the subject of an official Board of Enquiry (similar to rail and air disaster enquiries). A Board of Enquiry must have the power to make changes to the system under investigation and/or the methods, tools, products and staff associated with the certification procedure.

Any error triggers Board of Enquiry

B.21 Any error, no matter how 'small', in a software system which has been certified as being safe must be subject of an Enquiry. This is the only way of discovering weaknesses in the certification process itself, or misuse or misunderstanding of its application. Enquiries concerning non-fatal errors should not have disciplinary implications, so that operators are encouraged always to give notification of minor faults.

Near Miss

B.22 Any serious 'near miss' must be reported to the Licensing Authority. An Enquiry should be held if the Licensing Authority is concerned at the incident's implications.

Safety certification

B.23 The UK must develop the ability to certify safety aspects of software system construction and operation. These include:

* certification of the mathematical soundness of the methods of construction;

* certification that certified methods are properly applied during construction and subsequent maintenance (rectification and development);

* certification of the tools used during construction and maintenance;

* certification of the software engineers who build and maintain the systems;

* certification of the end product, that is, the software itself.

B.24 Methods should not be certified which are merely 'good practice'. Safety and reliability require more rigorous theoretical bases than

existing good practice, so that system behavior can be accurately and consistently predicted; hence the need for mathematical soundness to enable prediction to be based on mathematical proof.

B.25 Certification of a tool will only be given when it is shown that the tool preserves the mathematical soundness of the method is supports.

B.26 Certification of software engineers will only be given when they have completed an approved level of formal mathematical and methodological training together with an approved track record of experience. Certification should be of limited duration; recertification should require additional formal training both of the refresher type and new developments. Recertification should occur at regular intervals.

B.27 Certification of end products (and their components) implies proof obligations in addition to thorough testing. Proofs must be performed and checked by competent mathematicians or by a machine running certified software.

B.28 As in other branches of engineering, the rigour of the inspection procedures should be adjusted to the degree of risk, the severity of the danger and the cost. For example, we can imagine the emergence of several levels of certification:

a. Disaster Level. Failure could involve more than ten deaths. The whole of the software must be checked by formal mathematical proof, which is itself checked by a competent mathematician. Further precautions required if damage limitation by switch-off is not feasible (para B.15).

b. Safety Level. Where failure could cause one death, but further danger can be averted by switch-off. The whole of the software must be constructed by proof-oriented methods, checked by a competent mathematician. On occurrence of a fatality, the mandatory Enquiry must name the programmer and mathematician responsible, who might be liable for criminal negligence. Perhaps one error per 100,000 lines of code would be a realistic expectation, so that most shorter programs will contain no errors.

c. High Quality Level. Appropriate for software sold commercially, where error could bring financial loss to the customer. By law, such losses should be reimbursed. All programmers involved should be certified competent in mathematical methods of software design and construction. Their use of the methods is checked by sampling. An acceptable error rate would be one error per 10,000 lines of code delivered. Each error corrected requires recertification at Safety Level. If the target error rate is exceeded, certification is withdrawn. Eventually, all software used to construct other certified software should be certified to this level; and the construction of 'disaster level' software should include independent checks on the correct working of support software used (for example, check of binary code against higher level source codes).

d. Normal Quality. Corresponds roughly to the best of current practice (say, one error per 1,000 lines of code). The methods used to construct software to higher levels of reliability may also be used to achieve normal reliability; and this should bring a significant improvement

in programmer productivity and a reduction in the whole life cycle costs of the programs they produce.

Search RISKS using swish-e

THE RISKS DIGEST

Forum on Risks to the Public in Computers and Related Systems

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

Volume 4: Issue 15

Thursday, 20 November 1986

Contents

IBM VM/SP Cracked

Jack Shaw <JDS2F%UOTTAWA.BITNET@WISCVM.WISC.EDU>
Tue, 4 Nov 1986 22:32:40 EST

It appears someone (student hacker) has cracked VM. Anyone interested
in this should contact their IBM SE about APAR VM26824. Looks like
a pretty serious breach too...Hacker was able to change anyone's CP
class from A-H or their own CP class.

Jack Shaw, Univ. of Ottawa

On placing the blame and Safety-Critical UK Software (RISKS 4.14)

Bjorn Freeman-Benson <bnfb@beaver.cs.washington.edu>
Thu, 20 Nov 86 12:44:36 PST

I do not have a copy of the ACARD report, but judging from Appendix B,
this report attempts to put almost all the blame for computer failures
on the software, rather than the hardware, operation or the combined system.

>B.3 The fault lies not so much in the computer hardware as in the programs
>which control them, programs full of the errors, oversights, inadequacies
>and misunderstandings of the programmers who compose them...

Any system is only as strong as it's weakest link, and so any Certified software will have to be written, installed, run on and operated by Certifed people and machines. But, worse than that, what about interactions between the software and the hardware, or even other software (like the OS)? For example, Certified package A runs on Certified OS B on Certified hardware C. Something in C fails and B takes care of it, but in doing so response time falls until A fails (such as running a ship into an oil-rig).

Certifying software would be a big step forward, but I think that concentrating on just one part of the whole system will not safely Certify that system. For example, reread the past N RISKS where time after time an operator error has caused problems. Or look at the real experience that I based the previous example on:

> We had a PDP-11 (not Certified) in which a board failed sending an inordinate number of spurious interrupts to the CPU. The OS handled them all, but response time went down by 80%.

If the system failed that way, who would be held liable?

Bjorn

[First, we have been around this question on numerous occasions. There is often NO ONE PLACE TO PUT THE BLAME. Second, the ACARD report sets out to make a strong case for what the UK should do WITH RESPECT TO SOFTWARE. In that context, I don't think the report as a whole denies that other factors are not also critical; it just focuses on software. (The rest of the report is certainly of interest to software engineers. By the way, don't ask me about how to get copies. Ask HMSO. Perhaps one of our British correspondents can provide ordering information.) PGN]

Re: On placing the blame (Peter J. Denning, RISKS-4.14)

rutgers!meccts!mecc!sewilco@seismo.CSS.GOV <Scot Wilcoxon>
Thu, 20 Nov 86 11:35:24 EST

In the [first cited] example, the collision-avoidance method failed because the air traffic controller could not communicate with the aircraft. The present method cannot compensate for jammed radio frequencies, unless the aircraft are monitoring the international emergency channel and the controller thinks of trying it.

[Observation: Even though the jammed frequency is not a computer problem per se, it greatly impacts the ability of the computerized ATC system to do its job. PGN]

Other recent postings have pointed out the centralized characteristic of the existing collision-avoidance methods preferred by the FAA and compared them to an aircraft-based Honeywell system. The distributed Honeywell system has

the advantage of not depending upon the ground-based computer and communication with it.

The present system includes distributed jammers, one on board every aircraft.
Scot E. Wilcoxon Minn Ed Comp Corp {quest,dayton,meccts}!mecc!sewilco
(612)481-3507 sewilco@MECC.COM ihnp4!meccts!mecc!sewilco

Safety-Critical Software in the UK

"Scott E. Preece" <preece%mycroft@GSWD-VMS.ARPA>
Thu, 20 Nov 86 09:27:44 CST

The proposed regulation of safety-critical software in the U.K. is very interesting. What kind of status does the committee that wrote it have? Are these proposals that are likely to turn into law or are they just suggestions?

[This report comes from a very highly respected committee. After some debate, the proposals may very well get turned into law! PGN]

The notion of responsibility is a central element of the proposal. That's a very good thing. Everyone building systems should be thinking at all times that they are assuming responsibility for the use of their products. That responsibility should extend to anticipating the potential misuses of the system as well as to failures to perform to spec.

The proposed definitions at the end make it clear that this proposal is broader than it might first seem. They apparently propose to classify and, presumably, certify systems which endanger money as well as lives.

Defining the threat to life is, of course, non-trivial (shades of the 3+ laws of robotics). Would the administrative system implicated in the power-shutoff death reported here a few days ago have been considered life-critical? Would avionics systems for which non-automated, but less capable, backups are available? Is a program doing image enhancement on satellite pictures used by weather forecasters life-critical? How about the operating system it runs on?

scott preece, gould/csd - urbana, uucp: ihnp4!uiucdcs!ccvaxa!preece

---

Computer-based stock trading [Some repetition, some new things]

<rutgers!meccts!ems!adam@seismo.CSS.GOV>
Thu, 20 Nov 86 15:58:04 EST

December 1986 DISCOVER, v7 #12 p13:

"SCIENCE BEHIND THE NEWS"
"DID COMPUTERS MAKE STOCK PRICES PLUMMET?"

News item: On Thursday, Sept. 11, 1986, the Dow Jones industrial average dropped 86.61 points, to 1792.89 -- a 4.61 per cent plunge. A record 237.6

million shares changed hands. The next day 240.5 million shares were traded, and the Dow fell 34.17 more points. Though the decline on Black Thursday paled next to that of Black Friday, Oct. 28, 1929, when the Dow fell 38.33 points, or a whopping 12.82 pre cent, Wall Street was shaken, and it's still looking for the cause. The Securities Exchange Commission (SEC) is now investigating the possibility that computerized program trading may have been a contributing factor.

The decline actually began on Wednesday, Sept. 10, the day before the big drop. The bond market in London looked weak, which suggested that interest rates would remain high, and there were signs of impending inflation. As always, these indications of a slumping economy drove the price of stocks down.

But many analysts believe that the drop was accelerated (though not initiated) by computer-assisted arbitrage. Arbitrageurs capitalize on what's known as the spread: a short-term difference between the price of stock futures, which are contracts to buy stocks at a set time and price, and that of the underlying stocks. The arbitrageurs' computers constantly monitor the spread and let them know when it's large enough so that they can transfer their holdings from stocks to stock futures or vice-versa, and make a profit that more than covers the cost of the transaction.

The computer programs used by arbitrageurs are based on simple mathematical formulas that take into account the prices of stocks and futures, dividends, and interest rates. "It doesn't require you to have 20 megabytes," says John Barbanel, director of futures trading at Gruntal and Co. in New York. In fact, the math can be done on the back of an envelope. But by the time a trader could do the calculations for his entire portfolio, the market opportunity would've passed, the price of futures and stocks changed. With computers, arbitrageurs are constantly aware of where a profit can be made.

However, throngs of arbitrageurs working with the latest information can set up perturbations in the market. Because arbitrageurs are all "massaging" the same basic information, a profitable spread is likely to show up on many of their computers at once. And since arbitrageurs take advantage of small spreads, they must deal in great volume to make it worth their while. All this adds up to a lot of trading in a little time, which can markedly alter the price of a stock. If, say, the arbitrageurs see that the price of a future has dropped below the price of its underlying stock, they may buy futures and sell the stock, en masse. Although Barbanel emphasizes that arbitrage stabilizes the market over a period of weeks and months, it can cause a lot of volatility within a single day.

"Some trader on the floor of the New York Stock Exchange sees all the arbitrageurs selling at once and bringing down the value of stocks," so he sells too, says Hayne Leland, the director of Leland O'Brien Rubinstein Associates, a Los Angeles investment management firm. Heavy selling leads to more heavy selling -- and even lower stock prices. And the fast calculations of computers can only magnify these effects. Barbanel says that 20 per cent of the 86-point drop on Thursday may have come from computer-assisted arbitrage.

[A different item included in the same message noted that Standard&Poor now reports the S&P 500 index and S&P 100 composite stock price index every fifteen seconds instead of once each minute. (For those people who really like to think they are inside the action? In case you want to make your computer-program-based trading "more precise"?) PGN]

FAA's Role in Developing a Mid-Air Collision-Avoidance System

Chuck Youman <m14817@mitre.ARPA>
Thu, 20 Nov 86 16:01:28 -0500

There have been a couple of items in RISKS lately about mid-air collision-avoidance systems. The FAA's role in developing a mid-air collision-avoidance system was the subject of testimony presented at a Congressional hearing in September by a GAO official, Herbert R. McLure. A copy of his statement can be ordered from the GAO. The accession number is 131086. See RISKS 3-67 for their address. Some of the points Mr. McLure made in his testimony:

> Controversy still surrounds FAA's 1976 decision to pursue its own system rather than fund one that was being developed commercially. This controversy remains largely because the technical problems associated with developing FAA's system have proved to be much more complex and time-consuming than originally anticipated. Our work has shown, however, that FAA's decision was supported by the aviation community and that, while a number of technical problems have delayed the commercial availability of FAA's system, these problems have apparently been solved. Significant issues must still be addressed, however, during the testing and certification process before FAA's system is ready for commercial use.
>
> By the 1970's private industry was developing several different systems. After testing three, FAA decided that the Honeywell AVOIDS was the most promising, but even it had shortcomings. While the technical problems found with AVOIDS were correctable, the most serious shortcoming in all three systems FAA tested was that converging aircraft would only be warned of each other's proximity if they were both equipped with the system. Since no aircraft had AVOIDS, FAA surmised that a federal mandate would have been required to ensure that the system was installed in enough aircraft to provide an adequate level of protection.
>
> Conversely, commercial aircraft equipped with FAA's system, then called the Beacon Collision Avoidance System, or BCAS, would be warned of the proximity of all other aircraft having a transponder and would receive recommended collision-avoidance maneuvers if the other aircraft had an altitude encoder. Since over 100,000 aircraft, or about 65 percent of the air fleet, already had transponders, [. . .] FAA believed that its system would offer more immediate protection at less cost to the avaition community and that an adequate level of protection could be obtained without mandating the system's purchase by all aircraft owners. Polls of aircraft owner and user groups in 1976 and 1979 showed that FAA's decision held substantial aviation community support.
>
> Honeywell stopped development of its AVOIDS system soon after FAA decided to proceed with BCAS. In the intervening 10 years, FAA has encountered a number of technical problems that have slowed the development of its system, now called TCAS. In June 1981, FAA's Administrator announced that TCAS would be the national standard for mid-air collision avoidance, and

that the system would be operational nationwide by mid-1985 at the latest. While this announcement was overly optimistic, it now appears that the known technical problems with the system have been solved. Testing the system in an operational environment and certification are all that remain before at least one model of TCAS can be commercially produced.

FAA's involvement in TCAS research and development has been unusual in that it has been conducted in-house by FAA's TCAS program engineering group instead of by private industry. Through its Office of Airworthiness, certification of TCAS' effectiveness is also FAA's responsibility.

Some TCAS program officials felt that FAA's involvement in research and development has resulted in over-cautiousness by the Office of Airworthiness in the certification process, and that TCAS is being subjected to much more scrutiny than it otherwise would have been.

Another kind of problem involves product liability. FAA officials told us they are concerned that if a mid-air collision should occur because pilots follow a faulty TCAS resolution advisory, FAA may have to accept responsibility and liability for the collision. They also think the issue of product liability would have been a major concern for private industry if it had developed the system.

A more complete report is also available from GAO: "Air Safety: Federal Aviation Administration's Role in Developing Mid-Air Collision Avoidance Back-Up Systems," GAO/RCED-86-105FS, Accession number 129832, April 22, 1986.

A number of the comments I have seen seem to imply that it would still be possible to implement the Honeywell system. Since its development was stopped 10 years ago, I doubt it. Also, I don't think it is valid to criticize a decision because in retrospect in may not have been the "best" decision. I think the criteria should be whether the decision was reasonable based on the information that was available at the time the decision was made. Both alternatives were viewed as being technically feasible (and this appears to be correct even in retrospect).

An issue that I think we should be discussing in RISKS is whether it is appropriate for the same organization to develop and approve critical systems. I think some degree of organizational independence is an absolute requirement.

Charles Youman (youman@mitre.arpa)

Search RISKS using swish-e

Report problems with the web pages to the maintainer

Search RISKS using swish-e

THE RISKS DIGEST

Forum on Risks to the Public in Computers and Related Systems

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

Volume 4: Issue 16

Saturday, 22 November 1986

Contents

"Banking machine almost ruins love life of Vancouver couple"

mnetor!lsuc!dciem!msb@seismo.CSS.GOV <Mark Brader>
Fri, 21 Nov 86 14:28:20 est

VANCOUVER (CP) -- Automated banking machines could prove hazardous to your love life, as an unidentified Vancouver woman can testify.

The woman tried to use her banking card to get money from an automatic teller in Honolulu.

"But by the time the message went, via satellite, from Hawaii to the central computer in New Jersey, then via land line to Seattle and Vancouver, then back to Hawaii, the teller machines [sic] had gone past its allowable waiting time," says a credit union spokesman. The woman did not get any money but the credit union in Vancouver took the money out of her account.

When the woman learned her account had been debited $1,100, she accused her fiance of taking it.

The fiance moved out and the woman reported the theft to the police, who picked up the man for questioning. It took almost a month for the two banks involved to solve the problem. The couple has since reunited.

[Reproduced from the Toronto Star, November 20, 1986. Submitted to RISKS by Mark Brader. Glossary for foreign readers: a "credit union" is similar to a bank; $1,100 Canadian is about $800 US.]

2+2= ? (Risks of self-testing, especially with nonexistent tests)

<LINDSAY@TL-20B.ARPA>
Sat 22 Nov 86 19:18:45-EST

If another car cuts in front of mine, then I would usually be alert enough to take evasive action. But, suppose ! The day will come when I happen to be looking at the scenery, or when there is a patch of mud on the road: and then the two problems compound into something serious.

It is in just this compounding manner that minor events turn into major events.

Once upon a time, a friend of mine was using a microprogrammed box to process satellite images. One day, it seemed to be malfunctioning: and in fact, when he looked inside, some of the error-indication LEDs were glowing.

Naturally, he ran the hardware test suite. However, the suite indicated that all was well. And thus it came about that my friend investigated the suite - and found that although they had written it, and although he ran it, it wasn't there !

The tests had been written in the only language which the box had, namely, a pretty homebrew assembler for its (wide) microcode. The assembler gave rather difficult listings, and did not finish by giving a count of errors. As a result, 4 of the 8 tests had in fact never assembled, and the programmer hadn't noticed.

Now, the host machine had a downloader, and it had an idiotic property. When asked to download a file which did not exist, it would simply create a null file, and then download that. Pardon ? Did I hear the phrase "error message" ?

On top of all this, the box's loader did not set the memory to a known state (like, all zero) before loading a file.

Worse yet, all of the 8 tests started at the same address, and printed the same messages (e.g. "Test starting").

We therefore see how an operator could faithfully run tests 1 through 8 without ever knowing that in fact, tests 5, 6, 7 and 8 did not exist !

We can also blame the original programmer for never having simulated a hardware error, to see if the tests caught it. And where was his manager ? And where is he now - out building missile guidance systems, maybe ?

Re: Computer-based stock trading

<RMann%pco@HI-MULTICS.ARPA>
Fri, 21 Nov 86 14:51 MST

Computer arbitrage should be self-limiting, just as pre-computer arbitrage is self-limiting. The price differential between a future and the stock index tends to permit arbitrage to occur. The question is who profits and who loses ? Clearly, after one of the huge price moves in a stock, the last arbitrager will experience a loss. Too many losses and he exits the game. Thus we have one less computer trader. Eventually, the number of successful computer traders should be the number who don't experience losses, and the stock price moves we see should be limited to smaller percentage moves.

Why hasn't this occurred ? A couple answers suggest themselves. (1) Computer arbitrage is not to blame any more than human-speed arbitrage is to blame. (2) Volatility as is perceived is not there (the same percentage move now as in 1974 would be three times as much in a absolute stock move.) (3) Other factors which are hidden and not well understood.

Re: appendix to ACARD report

Nancy Leveson <nancy@ICSD.UCI.EDU>
21 Nov 86 16:26:19 PST (Fri)

I am somewhat concerned by the implication in the report that checking the software by formal mathematical proof is the answer to the safety problem.

Although I believe that mathematical proof and certainly mathematical analysis should play an important role in building safety-critical software, it alone certainly will not guarantee an acceptable level of risk. Putting aside technical questions of whether it can be accomplished at all (e.g. what if the software contains real numbers?), formal mathematical proof can be used to show only the consistency between the specification and the program (or between levels of specification). BUT most accidents involving software have not been caused by coding errors but rather by misunderstandings about what the software should have been doing at all or erroneous assumptions about the actions of the environment or the controlled system, i.e. specification errors. It is the things that are left out or forgotten that cause the most problems. Furthermore, mathematical proof of the software will not handle the cases where the accident occurs because of the interaction between the software and the controlled system -- the software was "correct" in the usual formal mathematical sense.

Safety is a system problem and one cannot guarantee software safety by looking only at the software or by mathematically proving properties of the software in isolation from the operation of the rest of the system.

Nancy Leveson

Some further thoughts on the UK software-certification proposals

Dave Platt <dplatt@teknowledge-vaxc.ARPA>
Fri, 21 Nov 86 10:28:33 PST

The proposals in the ACARD report seem to place a great deal of emphasis on mathematical proof-of-correctness of computer programs (and the tools used to build them). I wonder just how practical this is, given the current state-of-the-art in software construction and theory, and I have a few questions to toss out.

Disclaimer: I'm a [reasonably good] programmer, not a high-power computer-science theorist; my knowledge of the state-of-the-art in correctness proofs is fragmentary and badly out of date. If I speak from ignorance, please feel free to correct and enlighten me!

1) Are existing programming languages constructed in a way that makes valid proofs-of-correctness practical (or even possible)? I can imagine that a thoroughly-specified language such as Ada [trademark (tm) Department of Defense] might be better suited for proofs than machine language; there's probably a whole spectrum in between.

2) Is the state of the art well enough advanced to permit proofs of correctness of programs running in a highly asynchronous, real-time environment?

3) Will the compilers have to be proved mathematically correct also? or might something like the Ada compiler/toolkit validation be adequate?

4) The report seems to imply that once a system is proven correct/safe, it can be assumed to remain so (for the [limited] lifetime of its License to Operate) so long as maintenance is performed by a certified software engineer. Is this reasonable? My own experience is that _any_ patch or modification to a program, no matter how minor it may seem, has a pretty substantial chance of causing unwanted side effects and thus voiding the program's correctness. Seems to me that a life-critical system should be completely revalidated (if not necessarily recertified) after any change, and that changes should probably be made in the original programming language rather than by low-level patches.

5) Many of the program "failures" I've encountered in "stable" software have been due to unexpected inputs or unplanned conditions, rather than to any identifiable error in the program itself. Can any proof-of-correctness guard against this sort of situation?

6) What are the legal aspects of this sort of proposal, from the programmer's point of view? Anybody got a good source of Programmers' Malpractice insurance?

7) Are the error-rate goals suggested in the report (1 error per 100,000 lines of code, or even less?) reachable?

8) Military systems such as the SDI control software would appear to belong
to the "disaster-level" classification... will they be subject to this
level of verification and legal responsibility, or will they be exempted
under national-security laws? [Of course, if an SDI system fails,
I don't suppose that filing lawsuits against the programmer(s) is going
to be at the top of anybody's priority list...]

9) If the certified software engineer responsible for a particular
piece of life-critical code resigns or is reassigned, is it reasonable
to assume that another (equally-qualified) CSE could in fact take over
the job immediately (on an urgent-call-out basis, for example)?

I respect the committee's concern for this problem, but I wonder whether
they haven't focused too much on one aspect (software correctness) at
the expense of considering other aspects (hardware reliability, adequate
specification of operating conditions, interfaces to humans and external
physical control systems, etc.).

Dependable Computing and the ACM Communications

Peter G. Neumann <Neumann@CSL.SRI.COM>
Wed 19 Nov 86 19:40:40-PST

There is an announcement by John Rushby in the November 1986 issue of the
Communications of the ACM (pp. 1031-2) regarding the establishment of
Dependable Computing as a CACM department -- regarding systems that must
dependably satisfy certain critical requirements such as safety, fault
avoidance, and fault tolerance. This announcement is also noteworthy in
that it provides a concise, easily accessible summary of some generally
accepted terminology that contributors to RISKS would do well to observe and
practice, including the Melliar-Smith / Randell distinctions among faults,
failures, and errors. It is hoped that RISKS readers with serious technical
contributions may find this CACM department an appropriate printed medium.

Search RISKS using swish-e

THE RISKS DIGEST

Forum on Risks to the Public in Computers and Related Systems

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

Volume 4: Issue 17

Monday, 24 November 1986

Contents

Computer Risks and the Audi 5000

Howard Israel <HIsrael@DOCKMASTER.ARPA>
Sun, 23 Nov 86 23:49 EST

The 23 November 60-Minutes tore apart Audi, Inc. It seems that the Audi 5000 model (automatic transmission) has a terrible habit of accelerating when moved from PARK to either FORWARD or REVERSE. The problem has been denied by Audi. They blame driver error ("They step on the gas instead of the brake"). Of course this appears to only be a problem with drivers of the 5000 model, none of the other models has such poor drivers.

The "alleged" defect is blamed for about 250 known accidents, and at least one death. [See more below.]

The alleged causes of the alleged problem (I should have been an alleged lawyer) include 1) excessive pressure build-up in the transmission, 2) a faulty "vacuum" (not sure of the exact words ??) unit (which Audi has

voluntarily notified its customers needs replacement, or will result in "performance" problems), and 3) a faulty on-board computer.

Although Audi insists that they cannot find a problem with the car, an "independent" expert hired by a group of people that have all experienced problems with the car (there are enough victims out there that a self-help group was formed) actually demonstrated the gas pedal *visibly* moving downward when the car was put into gear causing the alleged surging.

Even some valet parking garages have posted signs that they will not accept the Audi 5000 with automatic transmissions.

Audi is so convinced that the problem is driver error that they have issued a recall notice to install a safety switch so that the driver could not change the gear unless pressure was on the brake.

Footnote: Three accidents have occurred similiar to the stated alleged problem that had the brake safety switch installed. Audi said that 2 of the cars had the switch improperly installed, and the third was unexplained.
[Clive Dawson recalled "driver error" being cited for the third case.]

This whole incident is reminiscent of the Ford Pinto fiasco.

The Federal Transportation Safety Board (??) is investigating.

Audi (The Art of Engineering) came out looking very bad. (But what else would you expect from 60 Minutes?)

Corporate responsibility appears very low. I would not be surprised if they came out with a corporate apology within a week (in time for the next broadcast) to try to save face.

Howard Israel

[It is unusual for RISKS to get four different reviews of the same TV program! Excerpts from the others follow, with moderator's effort to minimize duplication and achieve accuracy. PGN]

Excerpts-From: Brint Cooper <abc@BRL.ARPA>

Even while the driver (quite literally) stands on the brake pedal, the car roars ahead. One young woman ran over and killed her own three-year-old son.

The "idle stabilizer" was said to be responsible for keeping a minimum flow of fuel to the engine during idle when the brakes are applied. The idle stabilizer is either a part of a computer-controlled system or is controlled by an on-board computer; it wasn't clear which.

Audi denies that anything is wrong. Two Audi representatives appeared on camera to assert that they could find nothing wrong with the car. They even claimed that the motorists are stepping on the wrong pedal.

Brint

Excerpts-From: churd@labs-b.bbn.com <Charlie Hurd>

The cars have accelerated with enough force to punch through walls. Many of the cars have been totalled.

Audi has checked the cars in question and failed to find any defects. They claim that the drivers became confused and pressed on the gas pedal instead of the brake. The drivers (one of them a police officer trained to drive under extreme conditions) maintain that they were trying to put the brake pedal through the floor, without effect.

It seems to me that this is good response to Peter Stokes's question (RISKS-4.5) about the risks of buying/driving a car with a computer-controlled engine. The only question I have is why the brakes did not stop the car. Some of the victims said that they had to turn off the car to stop it. Do Audi 5000s have anti-skid braking? Could this have allowed the cars to keep moving? Is this an example of many small malfunctions resulting in a *major* problem?

Charlie

Excerpts-From: Clive Dawson <AI.CLIVE@MCC.COM>

This has resulted in at least one death. A young (6-year-old?) boy was let out of the car to open the garage door, after which the mother stepped on the brake and shifted to forward. The car hit the boy, pushed him completely through the garage door and pinned his already-crushed body against the rear wall of the garage. A heavy black skid mark was left which showed how even then the wheels continued to spin at a high rate of speed. The Audi people claim that all of these accidents are the result of driver error, in which the accelerator is mistaken for the brake. One of the more memorable quotes from Audi: "We're not saying we can't FIND anything wrong with the car; we're saying there ISN'T anything wrong with the car."

Attention is focusing on a microprocessor-controlled mechanism which regulates the idle speed. Apparently Audi has sent letters to all owners of the vehicles involved stating that this part will be replaced by Audi for "performance reasons". The report didn't make it clear whether the microprocessor was an integral part of this part or not, so I don't know if this replacement will involve a change in the processor or its software.

I don't know what the final verdict on this will be. But listening to that devastated mother tell how she witnessed the death of her son, and knowing the cause might eventually be tracked down to some software bug sent chills down my spine.

Clive

Risks of changing Air Traffic Control software?

Greg Earle <elroy!smeagol!earle@csvax.caltech.edu>

Fri, 21 Nov 86 22:47:04 pst

I haven't seen it mentioned yet, but I believe that last week I saw a news story that purported to blame a crash of a small light plane in the Southern California area on a changeover of software in either a radar system or a general flight controller computer system, causing either the plane to be lost from the screens or directed into a hillside. Since my memory is vague, perhaps someone else can provide a better recollection of this RISK of computer software.

Greg Earle, JPL

[The delay in running this item was due to an unsuccessful attempt to get further information... PGN]

Re: the UK Software-Verification Proposal

Bard Bloom <bard@THEORY.LCS.MIT.EDU>
Sun, 23 Nov 86 12:41:15 est

Disclaimer: I'm a grad student working in semantics of programming languages, and therefore qualified to pretend to know the answers to these questions. I haven't been studying semantics all that long, though. These are solely my opinions and bear no necessary resemblance to those of my advisor, my department, or my ceramic dragon.

> From: dplatt@teknowledge-vaxc.ARPA (Dave Platt) (RISKS 4.16)

> 1) Are existing programming languages constructed in a way that makes
> valid proofs-of-correctness practical (or even possible)? I can
> imagine that a thoroughly-specified language such as Ada [trademark
> (tm) Department of Defense] might be better suited for proofs than
> machine language; there's probably a whole spectrum in between.

No, they are not. Actually, there are a few existing programming languages (Euclid, for one) which are, but most popular ones are not. A precisely-specified language is easier to prove things about than an imprecisely-specified one, of course. I haven't seen anything approaching a precise mathematical semantics for Ada; if the research in semantics of distributed semantics goes very well we might be able to give you one in ten or fifteen years if we're lucky. The best languages for proving things about are functional languages (FP, Hope, Lucid, ISWIM). I have yet to hear of a "real program" written in any of these.

> 2) Is the state of the art well enough advanced to permit proofs of
> correctness of programs running in a highly asynchronous, real-time
> environment?

No. Not even remotely. We can't cope with slightly-asynchronous, non-real-time environments in any general way.

> 3) Will the compilers have to be proved mathematically correct also? or

> might something like the Ada compiler/toolkit validation be adequate?

The compiler will have to be proved too, if the idea of proving programs correct is to make any sense.

> 4) The report seems to imply that once a system is proven correct/safe,
> it can be assumed to remain so (for the [limited] lifetime of its
> License to Operate) so long as maintenance is performed by a
> certified software engineer. Is this reasonable? [...]

It is reasonable if you re-prove the patched system. I can't imagine it being reasonable otherwise. Note: you can probably patch the proof also, if it is arranged in a nicely modular form.

> 5) Many of the program "failures" I've encountered in "stable" software
> have been due to unexpected inputs or unplanned conditions, rather than
> to any identifiable error in the program itself. Can any proof-of-
> correctness guard against this sort of situation?

Not really. All the proof guarantees is that the software does what the specification does. That's a big help, since you don't usually have even that. But you have to get the specification right.

(I can't even pretend to answer questions about legal aspects.)

> 8) Military systems such as the SDI control software would appear to belong
> to the "disaster-level" classification... will they be subject to this
> level of verification and legal responsibility, or will they be exempted
> under national-security laws? [Of course, if an SDI system fails,
> I don't suppose that filing lawsuits against the programmer(s) is going
> to be at the top of anybody's priority list...]

That's a terrifying thought: don't verify Star Wars, it's too secret to have the code so exposed!

-- Bard Bloom

Program Trading

Howard Israel <HIsrael@DOCKMASTER.ARPA>
Sun, 23 Nov 86 23:49 EST [Other half of Howard's message]

Today's Washington Post, Sunday, November 23, 1986, pg K1 [Business Section] contains an interesting article on program trading and the Finance theory behind it all. (The following is partly based on the article and partly from my own knowledge.)

The basic idea is to view all of the different financial instruments as interrelated, even though the instruments may be traded on different markets across the country (or around the globe). The people that make it all work are called "Quants" (standing for Quantitative analyst). The "Quants" create models based on the markets and their

interelationships and known financial theory. When an "inefficiency" occurs (i.e., the price differential of an underlying security in two or more markets occurs that is big enough to cover the cost of the transactions involved), the computers that monitor the information issue simultanous buy and sell orders in the appropriate places. The net effect is the *total* elimination of risks once the initial set of transactions are complete (the winding up). (This is a simplification of it all. But the previous assertion in today's RISKS entry concerning the "last trader" losing money is not accurate.)

The profit is "locked in" when the first set of trades are completed, but will not be actually known until the positions are closed out (winding down) at the end of the finanical instruments life. The "published" profit margin is said to be in the 7% to 9% (annualized) range. (Anything above the current T-bill rate is considered good.) However, only each trader really knows what he is making. (A personal friend on "the street" claims that the profits are really much, much higher because the "invested money" stays in the market a very short time. I am not convinced of this based upon my knowledge of the trading --and "margin"-- necessary.)

The "Quants" differ from "Qualitative" traders, in that, Qualitative traders base their trades on the perceived quality of the companies (traditional recommendations of buy company ABC and sell company XYZ).

A nice analogy is made in the article to the gambling world. The "Quants" are the bookies, while the "Qualitative" traders are the River Boat Gamblers that bet on instinct.

Has anybody thought of the implications (since the computers, based on its programmed models and incoming data) of an error ? Not only is big money involved (it is estimated that one needs a *minimum* of $50 million to play the game), but so are bigger reputations (not just the brokerage houses, but insurance companies, too).

Is it "bad" for the market ? I think not. When the computer generated trades are executed they force market correction. The article makes a point that new financial instruments are emerging that will "play the game", much like a mutual fund does now for the small investor. These instruments will limit the "downside" loss, while maintaining unlimited "upside" gain. Then these new instruments can be used in conjuction with the already existing ones to create even more instruments, the end result, potentially being, that in time anyone can bet the market in any way.

---H

Re: RISKS DIGEST 4.16, Computer-based stock trading

<Nickell.pasa@Xerox.COM>
Sun, 23 Nov 86 19:33:07 PST

In response to Roger Mann:

(I mentioned this about a year ago in our last discussion of computerized stock markets.) Instantaneous and non-instantaneous negative feedback to not produce the same results. In this case, the fact that thousands of computers can respond to the possibility of profit before the effects of the responses get back (through whatever feedback loop) to any of them, opens the door for disaster.

Eric Nickell

Computer-based stock trading

<dmc%videovax.tek.csnet@RELAY.CS.NET>
Mon, 24 Nov 86 10:37:48 PST

The problem of decreasing system stability as time constants change is not a new one. Take the steam engine: "Watt's use of the flyball governor can be taken as the starting point for the development of automatic control as a science. The early Watt governors worked satisfactorily, no doubt largely due to the considerable amounts of friction present in their mechanism, and the device was therefore widely adopted. ... However, during the middle of the 19th century, as engine designs changed and manufacturing techniques improved, an increasing tendency for such systems to hunt became apparent; that is, for the engine speed to vary cyclically with time. ... This problem of the hunting of governed engines became a very serious one (75,000 engines, large numbers of them hunting!) and so attracted the attention of a number of outstandingly able engineers and physicists. It was solved by classic investigations made by Maxwell, who founded the theory of automatic control systems with his paper "On Governors," and by the Russian engineer Vyschnegradsky, who published his results in terms of a design rule, relating the engineering parameters of the system to its stability. Vyschnegradsky's analysis showed that the engine design changes which had been taking place since Watt's time - a decrease in friction due o improved manufacturing techniques, a decreased moment of inertia arising from the use of smaller flywheels, and an increased mass of flyball weights to cope with larger steam valves - were all destabilizing..."

"The Development of Frequency-Response Methods in Automatic Control", Alistair G. J. MacFarlane, IEEE Trans. Automat. Contr., pp. 250 - 265, Apr. 1979

Decision Making

Clive Dawson <AI.CLIVE@MCC.COM>
Mon 24 Nov 86 13:34:19-CST

Those interested in the recent item on the science of decision-making [see Jim Horning, "Framing of Life-and-Death Situations", Risks 4.13] might find this reference a bit more accessible:

"Decisions, Decisions", by Kevin McKean. DISCOVER Magazine, June, 1985.

This article is a well written account of the work done by a number of researchers, notably Daniel Kahneman and Amos Tversky, and has several very nice examples of how the framing of a question affects the decision making process.

Anybody who had trouble locating CMU's "1986 Accent on Research Magazine" would have better luck with Discover Magazine.

Search RISKS using swish-e

THE RISKS DIGEST

Forum on Risks to the Public in Computers and Related Systems

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

Volume 4: Issue 18

Wednesday, 25 November 1986

Contents

RISKS, computer-relevance, where-to-place-the-blame, etc.

Peter G. Neumann <Neumann@CSL.SRI.COM>
Tue 25 Nov 86 18:58:38-PST

This is another note on the risks of running RISKS. We get a variety of contributions that are not included in RISKS, on the grounds of relevance, taste, lack of objectivity, politicization, etc. (Once in a while I get a flame about censorship from someone whose message is not included, but I tend to stand by the masthead guidelines.) I also get an occasional complaint about my judgement regarding RISKS messages that have been included. So, it is time for some further comments from your moderator.

One of the most important things to me in running RISKS is that there is a social process going on, at many levels. First, there is an educational function, in raising the level of awareness in many computer professionals and students, whether naive or young, whether sophisticated or old. Second, there is a communications function of letting people try out their ideas in an open public forum. They also have an opportunity to become more responsible communicators -- combining both of those functions. Also, there

is the very valuable asset of the remarkably widespread RISKS community itself -- there is always someone who has the appropriate experience on the topic at hand. By the way, I try not to squelch far-out thinking unless it is clearly out of the guidelines. This sometimes leads to unnecessary thrashing -- although I try to minimize that with some of my [parenthetical] interstices.

The Audi case is one in which computer relevance is not at all clear. However, the presence of microprocessors indicates that it is worth our while discussing the issues here. The Audi problem is of course a total system problem (like so many other problems). I tend to include those cases for which there is a reasonable connection with computer technology, but not necessarily only those. There are various important issues that seem worth including anyway -- even if the computer connection is marginal. First, there are total systems wherein there is an important lesson for us, both technological and human. Second, there are total systems that are NOT AT PRESENT COMPUTER BASED or ONLY MARGINALLY COMPUTER BASED where greater use of the computer might have been warranted. (Nuclear power is a borderline case that is exacerbated by the power people saying that the technology is too critical [or sensitive?] for computers to be used. THEY REALLY NEED DEPENDABLE COMPUTING TECHNOLOGY. Besides, then THEY could blame the computer if something went wrong! -- see second paragraph down.)

There is an issue in computer-controlled automobiles (even if the computer is clearly "not to blame" in a given case) whether the increased complexity introduced by the mere existence of the computer has escalated the risks. But that is somewhat more subtle -- even though I think it is RISKS related...

The issue of simplistically placing blame on the computer, or on people (or on some mechanical or electrical part), or whatever, has been raised here many times. I would like all RISKS contributors to be more careful in not trying to seek out a single source of "guilt".

There are undoubtably a few people in our field who are bothered by technological guilt. There are others who are totally oblivious to remorse if their system were to be implicated in an otherwise avoidable death. However, the debates over blame, guilt, and reparation are also a part of the "total systems" view that RISKS tries to take.

I try not to interject too many comments and not to alter the intended meaning. However, what YOU say reflects on YOU -- although it also reflects on me if I let something really stupid out into the great Internet. Also, some discussions are just not worth starting (or restarting) unless something really new comes along -- although newer readers have not been through the earlier process, and that is worth something.

I have an awkard choice when a constructive contribution contains a value judgement that is somewhat off the wall. I sometimes edit the flagrant comments out, despite my policy of trying to maintain the author's editorial integrity. I thought for a while about Clive Dawson's "knowing the cause might eventually be tracked down to some software bug sent chills down my spine." The same could be said for the products of other technical professionals such as engineers and auto mechanics. (But that statement is a sincere statement of Clive's feelings, and this one was left in.)

[Apologies for some long-windedness. I probably have to do this every now and then for newer readers.] PGN

Verification and the UK proposal (RISKS 4.17)

Jim Horning <horning@src.DEC.COM>
Tue, 25 Nov 86 11:37:49 pst

I find myself largely in agreement with Bard Bloom's comments in RISKS 4.17. However, it seems to me that recent discussion has overlooked one of the most important points I saw in the UK proposal: verification is a way of FINDING errors in programs, not a way of absolutely ensuring that there are none. (The same is true of testing.)

Thus the kinds of question we should be asking are

- How many errors (in programs AND in specifications) can be found by presently available proof techniques? How many errors would be avoided altogether by "constructing the program along with its proof"?

- What is the cost per error detected of verification compared with testing? Does this ratio change as software gets larger? as the reliability requirements become more stringent?

- Do verification and testing tend to discover different kinds of errors? (If so, that strengthens the case for using both when high reliability is required, and may also indicate applications for which one or the other is more appropriate.)

- Can (partial) verification be applied earlier in the process of software development, or to different parts of the software than testing?

- Is there a point of diminishing returns in making specifications more complete? more precise? more formal? of having more independent specifications for a program?

I would dearly love to have convincing evidence that verification wins all round, since it would indicate that my work on formal specification is more valuable. But, to date, I haven't seen any convincing studies, and the arguments I can offer have been around for 10 or 15 years. (They look plausible. Why can't we prove them?)

Jim H.

When the going gets tough, the tough use the phone...

<LEICHTER-JERRY@YALE.ARPA>
25 NOV 1986 14:54:31 EST

or, Would you trust your teen-aged computer with a phone of its own?

From Monday's (24-Nov-86) New York Times:

Lyons, Ore., a town of about 875 people about 25 miles east of Salem, the state capital, has a small budget and a big problem. The monthly city budget is about $3,500. Back in October, the public library, with an annual budget of $1,000, installed a computer that made it possible to find a requested book at any library in the county through one telephone call to Salem.

After the trial run, no one knew that it was necessary to unplug the computer. It maintained the connection and ran up a bill of $1,328 with the Peoples' Telephone Company, the cooperative that runs the Lyons phone system.

"It leaves a problem I've got to figure out," said Mayor Jerry Welter. "I'm going before the phone company board to ask them to forgive the bill, and I don't know just how we'll manage if they won't do it."

Re: 60 minutes reporting on the Audi 5000

Eugene Miya <eugene@AMES-NAS.ARPA>
Mon, 24 Nov 86 22:43:49 pst

It's interesting -- the four perspectives collected on this telecast.

1) This was a subject broadcast several months ago on ABC 20/20. No mention on the microprocessor problem was made at that time, but the idle problem was demonstrated.

2) The microprocessor problem took very little time in the show, yet generated so much on RISKs (as it probably should).

3) I recall TWO deaths in the program, not just one, and probably more. Two correspondents pointed out the dead child, but the others did not mention the gas station attendent who was dragged underneath the car when it lurched backward over 200 feet. Five different views of the same show. (Rashomon) Could we expect a computer to do better? I hope so.

--eugene miya

Minireviews of Challenger article and a computerized-roulette book

25-Nov-1986 1808 <minow%bolt.DEC@src.DEC.COM>
Tue, 25 Nov 86 15:22:31 pst

"Letter from the Space Center" by Henry S. F. Cooper in the New Yorker, November 10, 1986, pp. 83-114. Discusses the Challenger accident and the way it was investigated. New (to me) information includes some things that were known to the engineers before the accident, but not taken into account when the decision to fly was made. There is also mention of a few things "hidden" in the appendices to the Presidential

Commission's report.

Nothing specific on computers, but a lot on the *management* of technological risks, and -- as such -- would be interesting reading to the Risks community.

Book: The Eudaemonic Pie, by Thomas A. Bass. Vintage Books (paper), Houghton-Mifflin (hardbound). ISBN 0-394-74310-5 (paper). Relates the engrossing tale of a bunch of California grad students who decided that roulette is "just" an experiment in ballistics (with a bit of mathematical chaos theory thrown in). Unfortunately, the adventurers were better physicists than engineers and their computer system, built into a pair of shoes, never worked well enough to break the bank. They had some good moments, though. The physicists went on to more and better things, and have just published an article on chaos in the current Scientific American.

Martin

More on the UK Software-Verification Proposal

Bill Janssen <janssen@mcc.com>
Tue, 25 Nov 86 18:09:22 CST

> Bard Bloom in RISKS 4.17:

> 1) Are existing programming languages constructed in a way that makes
> valid proofs-of-correctness practical (or even possible)? I can
> imagine that a thoroughly-specified language such as Ada [trademark
> (tm) Department of Defense] might be better suited for proofs than
> machine language; there's probably a whole spectrum in between.
> 2) Is the state of the art well enough advanced to permit proofs of
> correctness of programs running in a highly asynchronous, real-time
> environment?

Drs. K. Mani Chandy and Jayadev Misra of the University of Texas at Austin have developed a language called UNITY, which allows one to write programs for distributed asynchronous systems, and reason about the relationship between the program and its specification, which may allow one to prove that the program correctly implements the spec. (More often, one proves it does not...) At least one compiler for UNITY exists.

[Further discussion on this probably belongs in Soft-Eng@XX.MIT.EDU. (See also various papers by Leslie Lamport.) But I let this one through because proving properties of asynchronous programs is generally a very high-risk area. Many asynchronous algorithms widely thought to be "correct" or "safe" or whatever are not... PGN]

Report problems with the web pages to the maintainer

Search RISKS using swish-e

THE RISKS DIGEST

Forum on Risks to the Public in Computers and Related Systems

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

Volume 4: Issue 19

Wednesday, 26 November 1986

Contents

Very Brief Comments on the Current Issues

"Kim P. Collins" <kpc%duke.csnet@RELAY.CS.NET>
Wed, 26 Nov 86 13:32:05 EST

Verification

It seems to me that there are a priori limits to the usefulness of verification for software engineering. To prove that a program will work, even with the best system, is no doubt a non-trivial process, and hence subject to some of the same problems that the software design process has.

Relevance of contributions

I think that we need not have computers involved for contributions to be relevant. I see the limits being only those things that definitely belong elsewhere. Computer science is a cybernetic science and a science of cybernetics. Cybernetics covers a lot.

Audi 5000

The car must be incredibly powerful, or its control system INCREDIBLY unstable, to have caused so much damage. From an engineering perspective, assuming that it is not human error that is causing these occurrences, it seems that the unwise thing was to use an active control system (hence a risky one) with such a powerful machine.

New subject

Any comments on active vs. passive control structures? For instance, having a skyscraper that has flexible material so that in high winds it bends and does not fail, VS having a skyscraper that has guy wires connected to winches that are controlled by a computer that tests wind velocities, etc.

My opinion is that ceteris paribus (and even ceteris non paribus in many cases) passive control structures are to be trusted and used far more than active control structures. With active control structures, there are far more layers of abstraction and far more theories, designs, and sometimes materials that can fail. (Other reasons exist.)

Computerization of nuclear power plants

Computers can reduce the risks of cognitive overload and other human problems, but they also have some of the problems raised above. One advertisement by Carolina Power and Light during the most heated part of the Shearon Harris plant controversy here in NC said that the plant here would fail by dint of gravity in a relatively safe manner. The plant in Chernobyl, it said or implied (I don't remember which), would not. This is the active/passive control structure dichotomy applied to one particular part of the computerization of a nuclear plant. I think that we need to look at the different parts during the design stage and make certain that we minimize the active. (No opinion on nuclear power is intended here.)

CSNET: kpc@duke, UUCP: {ihnp4!decvax}!duke!kpc

The Audi discussion is relevant

<Murray.pa@Xerox.COM>
Wed, 26 Nov 86 17:09:20 PST

"The Audi case is one in which computer relevance is not at all clear."

It seemed quite relevant to me on two grounds.

First, adding a computer to an automobile is an important social experiment, even if Audi didn't know they were taking part in one. I can't think of any other application where people who probably don't know much about computers are now depending upon computers as part of a large complicated system where errors can easily kill people. I don't watch TV, so I'm pleased to see that sort of information in RISKS.

The second aspect is the normal computer engineering problem (in a high

risk situation). I would like to know what went wrong. Hardware? Software? System integration? Specification oversight? .... It's probably a small computer and thus not very exciting relative to big systems with megabytes of memory and millions of lines of code. Since the results of a problem have been demonstrated to be very important (to at least a few people), I think we should investigate this case in hopes of learning something. Maybe it will even be easier to analyze because the computer part of the system is so small.

Audi 5000

Roy Smith <allegra!phri!roy@ucbvax.Berkeley.EDU>
Wed, 26 Nov 86 00:23:49 est

I also saw the 60 Minutes episode. From the tone of the various messages in RISKS 4.17, it sounds like everybody believes Audi is at fault. All I saw was a lot of anecdotal evidence and a lot of people who seem to think that if they say something often enough and with enough emotion, it will become true. Lacking any real facts, I can't begin to make up my mind what the answer is. I'm certainly not going to decide based on the 60 Minutes testimony of a woman who ran over her own son. This is admittedly a terrible thing to happen, but why should we give her claim that she had her foot on the brake pedal any more or less credence than the claims of the Audi engineers? A comment:

> Clive Dawson <AI.CLIVE@MCC.COM>
> One of the more memorable quotes from Audi: "We're not saying we can't FIND
> anything wrong with the car; we're saying there ISN'T anything wrong with
> the car."

Indeed, this is such a patently stupid thing to say that I'm now almost *convinced* that there must be something wrong with the car. Any company that could hire somebody that would say something so absurd must have problems. Imagine somebody telling you "I'm not saying we can't FIND any bugs in the SDI system, I'm telling you there AREN'T any." :-)

Roy Smith, {allegra,cmcl2,philabs}!phri!roy
System Administrator, Public Health Research Institute
455 First Avenue, New York, NY 10016

Laser-printer health risks; also, how to get ACARD report

Jonathan Bowen <bowen%sevax.prg.oxford.ac.uk@Cs.Ucl.AC.UK>
Wed, 26 Nov 86 15:22:08 GMT

Front page headlines from Computer News, 20 November 1986:

`Health risk fears spur CCTA to probe laser standards'

`Fears over laser printers have spurred the government's computer purchasing agency into questioning health and safety standards. The Treasury's Central

> Computer and Telecommunications Agency (CCTA) has said it will investigate
> claims that the printers can cause chest infections, blindness and other
> serious health problems. Already one major UK user, British Rail (BR), has
> delayed a decision on buying printers because of a lack of published safety
> standards.
> ....leading laser printer-makers Apple, Hewlett-Packard and Xerox
> denied their products could be harmful.
> ....A senior CCTA official said: "We have looked at lasers...they
> can cause temporary blindness to some people."
> ....white collar union Apex, said: "...Many of our members within
> the industry have reservations about the safety of laser printers."
> Already the use of laser printers has caused a three-day strike
> by Danish postal workers until they were given safety assurances
> by the government.
> A report from a leading Danish laboratory has said damage to the
> retina and lungs can be caused by laser printers.
> ...In 1981, IBM voluntarily withdrew one substance, trinitroflurenone (TNF),
> which was a photoconductor constituent in its Model 1 3800 laser printer.
> An IBM spokesman said: "We established it had a potential to be harmful,
> although not in the way we were using it."'

Is this going to be the same sort of scare as that associated
with VDUs? Has anyone else heard of these problems? Are there
appropriate safety standards in the US or elsewhere?

By the way, for anyone interested in the ACARD report, here is
an HMSO address:

> Her Majesty's Stationery Office, PO Box 276, London SW8 5DT, England
> Tel +44-1-622-3316

The cost of the report is 6 pounds. The HMSO will invoice you if
you apply to the above address. (Be prepared to pay in pounds.)

Jonathan Bowen

Data point on error rate in large systems [Grapevine rot?]

<Murray.pa@Xerox.COM>
Wed, 26 Nov 86 18:55:35 PST

Grapevine is the mail system used by the Xerox R+D community. It has been
operational since 1981. Currently, there are 21 servers and roughly 4000
users. The servers have accumulated roughly 75 server-years of up time.

This spring, we discovered a fatal bug in the server code. It's been there
from the start. It was a simple recursive error in a very unlikely case.
Because the case was also uninteresting, nobody had bothered to "try it".

Fine print, if anybody cares:

The Grapevine database has two types of entries: groups and individuals. An

individual is normally a person who reads/sends mail. A group is normally a distribution list or an access control list. The members of a group can be either individuals or other groups. Aside from the membership list, a group also has a list of owners. The owners of a list are allowed to update it. There are also pseudo groups. If you send a message to "Owners-xxx", the system distributes the message to the owners (rather than members) of xxx.

Since a group can have members that are groups, there is the obvious recursive problem. To check for this, the code that expands the membership of a group runs up the call stack to see if another instance of itself is already expanding this group. Unfortunately, the code that processed Owners-xxx asked if anybody was already expanding xxx, while they all thought they were working on Owners-xxx. Thus if Owners-xxx was an owner of xxx, and anybody asked if Joe was an owner of xxx, poof.

PS: Mike Schroeder told me that they used to discover a new horrible bug/oversight roughly every time the size of the system doubled.

Re: Program Trading

<RMann%pco@HI-MULTICS.ARPA>
Wed, 26 Nov 86 13:48 MST

I apologize to anyone for carrying this on further, but I am still not convinced that computers are creating the wide stock price swings that we see today in the market. Assuming a model of some sort that detects "inefficiencies", there must be a range of stock or option or futures for which the inefficiency holds. Beyond those thresholds, the no-lose situation does not exist and should be avoided.

Now I am a dabbler in stocks and I know about limit orders. Limit orders are filled if the price of the stock is below a certain price on a purchase or if the price is above a certain price on a sale. This is extremely useful when trying to establish a hedged position. Now, I can't imagine these super-sophisticated arbitrageurs issuing MARKET orders -- it is too absurd to imagine. If the hedger issues limit orders, the trades do not occur and the stock price stays relatively stable.

Now, is there anyone out there who has direct knowledge of these things and is willing to spill the beans and give us the straight scoop ? Are computers the risk here or not ?

Technical merits of SDI

Peter G. Neumann <Neumann@CSL.SRI.COM>
Wed 26 Nov 86 13:22:31-PST

The following note from Richard A. Scribner, Committee on Science, Arms Control and National Security at the AAAS may be of interest to RISKS readers.

A detailed discussion of the technical merits of SDI, particularly software,

will be held as part of the First Annual AAAS Colloquium on Science, Arms Control, and National Security, 4-5 December 1986 in Washington DC. Among the distinguished speakers will be Lt.Gen. James Abrahamson, director of SDIO; James R. Schlesinger, Center for Strategic and International Studies; William Graham, science advisor to the President; Adm. Noel Gayler; Albert Carnesale, Dean of the Kennedy School of Government at Harvard; Dante Fascell, chairman of the House Committee on Foreign Affairs and chairman of the House subcommittee on arms control; Kosta Tsipis, director of the MIT Program on Science and Technology for International Security. For information and registration details, please call the American Association for the Advancement of Science at 202-326-6490.

Search RISKS using swish-e

Report problems with the web pages to the maintainer

Search RISKS using swish-e

THE RISKS DIGEST

Forum on Risks to the Public in Computers and Related Systems

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

Volume 4: Issue 20

Sunday, 30 November 1986

Contents

Smart metals

"Steven H. Gutfreund" <GUTFREUND%cs.umass.edu@RELAY.CS.NET>
Fri, 28 Nov 86 15:04 EDT

In Risks V4.19 Kim Collins calls for a discussions of passive versus dynamic control mechanism, and illustrates his definition with a skyscraper analogy:

> Passive Control: a building that flexes in the wind
> Dynamic Control: computer-controlled guy wires

With the advent of cheap 'smart' metals, (metals that contract or perform other mechanical functions in response to temperature and other environmental stimuli), is the distinction very important anymore? I can use a metal with complex operational characteristics to control the windows and blowers in my greenhouse and provide environmental control. The proper application and installation of these metal control structures seems directly analogous the the proper declaration of the constraints that a software control system should carry out. Indeed I can conceive of a modeling system for a completely software based control system that uses a graphics environment that expresses these contraints visually in terms of their mechanical counterparts: (e.g.

ThingLab or Maureen Stone's "Snap Dragging" in the SIGGRAPH '86 proceedings).

Let me phrase this in terms of a RISKS administration dilemna:

> If an engineer designs a control system in such a graphic modeling environment and has no knowledge whether the final implementation will be in terms of hardware (relay-ladder control, smart metals, etc) or in software. If his system fails and is submitted to RISKS, would the editor of RISKS consider this material valid RISKS DIGEST material if the final implementation was completely free of software and computers?
>
> - Steven Gutfreund
> University of Massachusetts, Amherst
>
> [You bet. An algorithm is an algorithm is an algorithm. Although it is not stated explicitly in the masthead, I consider this forum to be devoted to something like RISKS TO THE PUBLIC IN COMPUTER-RELATED TECHNOLOGIES, although don't ask for a specific definition of scope. Nice example. Thanks. PGN]

Risks of billing information on all telephone calls

Peter G. Neumann <Neumann@CSL.SRI.COM>
Sun 30 Nov 86 14:47:25-PST

> Sunnyvale CA (AP, 29 Nov 86) A telephone bill has vindicated a physically handicapped teenager jailed more than a month ago on charges he beat his mother to death. Charges were dismissed against Patrick Sparks, 17, when the bill found by his brother, Brad, 30, indicated their mother was still alive when the youth left home on the morning of the slaying, police said...

Of course, it can work either way. The record of all of your telephone calls provides a remarkable chronicle of your activities...

Audi and 60 Minutes

<mnetor!lsuc!dciem!msb@seismo.CSS.GOV>
Thu, 27 Nov 86 17:20:43 est

> I also saw the 60 Minutes episode. From the tone of the various messages in
> RISKS 4.17, it sounds like everybody believes Audi is at fault. All I saw
> was a lot of anecdotal evidence ...

That's all you *saw* because anecdotes make good pictures. If you listened to the "text" of the article, you heard statistics on the number of runaway Audis -- if I remember rightly, something like 1 in 300 owners of the model in question had experienced this problem. While they didn't give the "control statistic", the same ratio for other cars, I can't believe it's anywhere near that high -- can you?

Mark Brader, utzoo!dciem!msb

... being sysadmin of such a central node involves a lot less
hassle and frustration when I can confidently say, "I don't know
whose software is broken, but it definitely is not ours."
Speaking of which... "I don't know whose software is broken, but
it definitely is not ours!" -- Henry Spencer

Audi 5000/Micros in cars and the Mazda RX7.

Peter Stokes <stokes%cmc.cdn%ubc.csnet@RELAY.CS.NET>
Thu, 27 Nov 86 08:58:31 pst

[...]
I have heard that the new Mazda RX7's have microprocessor controlled steering
or something of the like. I guess this is the beginning of "drive by wire".
Peter Stokes, CMC

Automated trading

Scott Dorsey <kludge%gitpyr%gatech.csnet@RELAY.CS.NET>
Fri, 28 Nov 86 22:09:50 est

In the last Risks Digest, RMann%pco@HI-MULTICS.ARPA says:
"Now, I can't imagine these super-sophisticated arbitrageurs issuing MARKET
orders -- it is too absurd to imagine. If the hedger issues limit orders,
the trades do not occur and the stock price stays relatively stable."

Presumably the problem is not that of sophisticated arbitrageurs making
orders on enormous numbers of stock, but many thousands of not-so-sophisticated
people using computers for small market orders. With the advent of modern
services, practically anyone with a Commodore-64 can make predictions and
issue remote buy and sell orders. It's a strange world.

[And if they are all using the same program,
the effects can be even stranger. PGN]

"Borrowed" Canadian tax records; Security of medical records

<mnetor!lsuc!dciem!msb@seismo.CSS.GOV>
Thu, 27 Nov 86 17:19:18 est

Discussion has been going on in can.general about the "Borrowed" Canadian
income tax records, and the topic of security of medical records has arisen
as a sideline. I thought these two articles contained material good for RISKS.

Glossary for foreign readers: OHIP is the Ontario Health Insurance Plan.
Essentially all Ontario residents have coverage, but unless our income
is small, we (or our employers) have to pay a premium for it.

Mark Brader

========== Begin 1st forwarded article ==========
Path: dciem!utzoo!mnetor!spectrix!clewis
From: clewis@spectrix.UUCP (Chris Lewis)
Newsgroups: can.general
Subject: Re: Borrowed records from Revenue Canada
Date: 26 Nov 86 21:05:24 GMT

In article <274@cognos.UUCP> glee@cognos.UUCP (Godfrey Lee) writes:
>Did anyone see the news report that the suspect "has opened"/"wants to open"
>an agency to track down people for a fee?

[Interpolation by Mark Brader: Another report was that he wanted to use the records to reunite people with their forgotten bank accounts, for a fee. Of course, he could have been planning both things.]

Oops, forgot about that one. Yes, indeedy, it would be good for "skip tracing". Interestingly enough, in Ontario, the OHIP enrollment file is even better - the dates are frequently far more up to date, because even tax avoiders (and others attempting to avoid payments) want to keep their OHIP coverage up-to-date. Until 1978/9 police were able to obtain such information - the general manager of OHIP didn't realize that the legislation enabling the existence of OHIP didn't allow it. Not any more. However, there were far more private investigators using pretext calls to OHIP for the same end.

As an example of where things are compared to what they were like in 1978 (when the Health Records Commission started), OHIP didn't know how many copies of the OHIP enrollment fiche were made, where they went and never noticed any going missing (quite a few copies did - though, most likely they were simply misplaced or destroyed without being reported to the COM group).

One of the more interesting (and sneaky) techniques we ran into for collection agencies acquiring info was:

1) Send letter saying "You have won....(something or other)" along with a cheque for $5 "Deposit Only" to debtor.
2) Find out the name of the debtor's bank from the cancelled cheque.

I was asked to report a few other incidents that the Commission found:

1) Catastrophic OHIP data processing oversight:

It is the practise of OHIP to collect several days worth of data entry at one of their district offices (there were 7 in 1978-79) and do an audit on them. Once every couple of months. This is done by taking the several days worth of claims (in the order of 100,000-400,000 claims) and running them through a program that would generate a letter of the form:

Dear

Search RISKS using swish-e

THE RISKS DIGEST

Forum on Risks to the Public in Computers and Related Systems

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

Volume 4: Issue 21

Sunday, 30 November 1986

Contents

Risks of Computer Modeling and Related Subjects (LONG MESSAGE)

"John Michael (Mike) Williams" <JWilliams@DOCKMASTER.ARPA>
Fri, 28 Nov 86 13:02 EST

Taking the meretricious "con" out of econometrics and computer modeling:
"Con"juring the Witch of Endor
John Michael Williams, Bethesda MD

Quite a few years ago, the Club of Rome perpetrated its "Limits to Growth" public relations exercise. Although not my field, I instinctively found it bordering on Aquarian numerology to assign a quantity, scalar or otherwise, to "Quality of Life," and a gross abuse of both scientific method and scientific responsibility to the culture at large. Well after the initial report's firestorm, I heard that a researcher at McGill proved the model was not even internally consistent, had serious typographical/syntactical errors that produced at least an order of magnitude error, and that when the errors were corrected, the model actually predicted an improving, not declining "Quality of Life." I called the publisher of "Limits to Growth," into its umpteenth edition, and asked if they intended to publish a correction or retraction. They were not enthusiastic, what with Jerry Brown, as Governor and candidate for Presidential nomination, providing so much lucrative publicity. Jimmy Carter's "malaise" and other speeches suggest that these dangerously flawed theses also affected, and not for the better, both his campaign and administration.

This shaman-esque misuse of computers embarrassed the computing community, but with no observable effect.

On 31 October 1986, Science ran a depressing article entitled: "Asking

Impossible Questions About the Economy and Getting Impossible Answers" (Gina Kolata, Research News, Vol. 234, Issue 4776, pp. 545-546). The subtitle and the sidebar insert are informative:

> Some economists say that large-scale computer models of the economy are no better at forecasting than economists who simply use their best judgment... "People are overly impressed by answers that come out of a computer"...

Additional pertinent citations (cited with permission):

> "There are two things you would be better not seeing in the making--sausages and econometric estimates," says Edward Learner, an economist at [UCLA]. These estimates are used by policymakers to decide, for example, how the new tax law will affect the economy or what would happen if a new oil import tax were imposed. They are also used by businesses to decide whether there is a demand for a new product. Yet the computer models that generate these estimates, say knowledgeable critics, have so many flaws that, in Learner's words, it is time to take the "con out of econometrics."
>
> ...[E]ven the defenders of the models... [such as e]conomists Kenneth Arrow of Stanford and Stephen McNees of the Federal Reserve Board in Boston say they believe the models can be useful but also say that one reason the models are made and their predictions so avidly purchased is that people want answers to impossible questions and are overly impressed by answers that come out of a computer...
>
> The problem, says statistician David Freedman of the University of California at Berkeley, is that "there is no economic theory that tells you exactly what the equations should look like." Some model builders do not even try to use economic theory...: most end up curve-fitting--a risky business since there are an infinite number of equations that will fit any particular data set...
>
> "What you really have," says William Ascher of Duke University, "is a man-model system." And this system, say the critics, is hardly scientific. Wassily Leontief of New York University remarks, "I'm very much in favor of mathematics, but you can do silly things with mathematics as well as with anything else."
>
> Defenders of the models point out that economists are just making the best of an impossible situation. Their theory is inadequate and it is impossible to write down a set of equations to describe the economy in any event... But the critics of the models say that none of these defenses makes up for the fact that the models are, as Leontief says, "hot air." Very few of the models predict accurately, the economic theory behind the models is extremely weak if it exists at all, in many cases the data used to build the models are of such poor quality as to be essentially useless, and the model builders, with their subjective adjustments, produce what is, according to Learner, "an uncertain mixture of data and judgment."

When David Stockman made "subjective adjustments," he was reviled for cooking the numbers. It seems they may have been hash to begin with.

> [Douglas Hale, director of quality assurance at the (Federal) Energy

> Information Administration] whose agency is one of the few that regularly assess models to see how they are doing, reports that, "in many cases, the models are oversold. The scholarship is very poor, the degree of testing and peer review is far from adequate by any scientific measure, and there is very little you can point to where one piece of work is a building block for the next."
>
> For example, the Energy Information Administration looked at the accuracy of short-term forecasts for the cost of crude oil... At first glance, it looks as if they did not do too badly... But, says Hale, "what we are really interested in is how much does the price change over time. The error in predicting change is 91%"

This is about the same error, to the hour, of a stopped clock.

In the Washington Post for 23 November 1986, pg K1 et seq., in an interview entitled "In Defense of Public Choice," Assar Lindbeck, chairman of the Swedish Royal Academy's committee for selecting the Nobel Prize in economics, explains the committee's choice of Professor James M. Buchanan, and is asked by reporter Jane Seaberry:

> It seems the economics profession has come into some disrepute. Economists forecast economic growth and forecasts are wrong. The Reagan administration has really downplayed advice from economists. What do you think about the economics profession today?

Chairman Lindbeck replies:

> Well, there's something in what you say in the following sense, I think, that in the 1960s, it was a kind of hubris development in the economic profession ... in the sense that it was an overestimation of what research and scientific knowledge can provide about the possibilities of understanding the complex economic system. And also an overestimation about the abilities of economists to give good advice and an overestimation of the abilities of politicians and public administrators to pursue public policy according to that advice.
>
> The idea about fine tuning the economy was based on an oversimplified vision of the economy. So from that point of view, for instance, economists engaged in forecasting--they are, in my opinion, very much overestimating the possibilities of making forecasts because the economic system is too complex to forecast. Buchanan has never been engaged in forecasting. He does not even give policy advice because he thinks it's quite meaningless...

What econometric computer model is not "an oversimplified vision of the economy?" When is forecasting an "economic system ... too complex to forecast" not fortune-telling?

To return to Kolata's article:

> [Victor Zarnowitz of the University of Chicago] finds that "when you combine the forecasts from the large models, and take an average, they are

> no better than the average of forecasts from people who just use their best judgment and do not use a model."

I cannot resist noting that when a President used his own judgment, and pursued an economic policy that created the greatest Federal deficit in history but the lowest interest rates in more than a decade, the high priests of the dismal science called it "voodoo economics." It takes one to know one, I guess.

> Ascher finds that "econometric models do a little bit worse than judgment. And for all the elaboration over the years they haven't gotten any better. Refining the models hasn't helped." Ascher says he finds it "somewhat surprising that the models perform worse than judgment since judgment is actually part of the models; it is incorporated in when modelers readjust their data to conform to their judgment."

Fascinating! Assuming the same persons are rendering "judgments," at different times perhaps, it implies that the elaboration and mathematical sophistry of the models actually cloud their judgment when expressed through the models: they appear to have lost sight of the real forest for the papier-mache trees.

> Another way of assessing models is to ask whether you would be better off using them, or just predicting that next year will be like this year. This is the approach taken by McNees... "I would argue that, if you average over all the periods [1974-1982] you would make smaller errors with the models [on GNP and inflation rates] than you would by simply assuming that next year will be just like this year," he says. "But the errors would not be tremendously smaller. We're talking about relatively small orders of improvement."

I seem to recall that this is the secret of the Farmer's Almanac success in predicting weather, and that one will only be wrong 15% of the time if one predicts tomorrow's weather will be exactly like today's.

> Other investigators are asking whether the models' results are reproducible... Suprisingly the answer seems to be no. "There is a real problem with scholarship in the profession," says Hale of the Energy Information Administration. "Models are rarely documented well enough so that someone else can get the same result..."
>
> [In one study, about two-thirds of the] 62 authors whose papers were published in the [J]ournal [of Money, Credit and Banking]... were unwilling to supply their data in enough detail for replication. In those cases where the data and equations were available, [the researchers] succeeded in replicating the original results only about half the time...

What a sorry testament! What has become of scientific method, peer review?

> "Even if you think the models are complete garbage, until there is an obviously superior alternative, people will continue to use them," [McNees] says.

Saul, failing to receive a sign from Jehovah, consulted a fortune-teller on the

eve of a major battle. The Witch of Endor's "model" was the wraith of Samuel, and it wasn't terribly good for the body politic either. I keep a sprig of laurel on my CRT, a "model" I gathered from the tree at Delphi, used to send the Oracle into trance, to speak Apollo's "truth." I do it as amusement and memento, not as talisman for public policy. History and literature are filled with the mischief that superstition and fortune-telling have wrought, yet some economic and computer scientists, the latter apparently as inept as the Sorcerer's Apprentice, are perpetuating these ancient evils. Are Dynamo and decendents serving as late-twentieth-century substitutes for I Ching sticks?

Is the problem restricted to econometrics, or is the abuse of computer modeling widespread? Who reproduces the results of weather models, for instance? Who regularly assesses and reports on, and culls the unworthy models? Weather models are interesting because they may be among the most easily "validated," yet there remains the institutional question: when the Washington Redskins buy a weather service, for example, to predict the next game's weather, how can they objectively predetermine that they are buying acceptable, "validated" modeling rather than snake oil? After all, even snake oil can be objectively graded SAE 10W-40, or not. A posteriori "invalidation" by losing while playing in the "wrong" weather is no answer, any more than invalidation by catastrophic engine failure would be in motor oils. The Society of Automotive Engineers at least has promulgated a viscosity standard: what have we done?

Where is scientific method at work in computer modeling? When peer review is necessarily limited by classification, in such applications as missile engagement modeling and war gaming, what body of standards may the closed community use to detect and eliminate profitable, or deadly, hokum? Is this just one more instance of falsified data and experiments in science generally, of the sort reported on the front page of the Washington Post as or before it hits the journals? (See: "Harvard Researchers Retract Published Medical 'Discovery;'" Boyce Rensberger, Washington Post, 22 November 1986 pg 1 et seq.; and Science, Letters, 28 November 1986.)

Several reforms (based on the "publish or perish" practice that is itself in need of reform) immediately suggest themselves. I offer them both as a basis for discussion, and as a call to action, or we shall experience another aspect of Limits to Growth-- widespread rejection of the contributions of computer science, as a suspect specialty:

o Refusal to supply data to a peer for purposes of replication might result in the journal immediately disclaiming the article, and temporary or permanent prohibition from publication in the journal in question.

o Discovery of falsified data in one publication resulting in restriction from publication (except replies, clarification or retraction) in all publications of the affiliated societies. In computer science, this might be all IEEE publications at the first level, AFIPS, IFIPS and so on.

o Widespread and continuing publication of the identities of the authors, and in cases of multiple infractions, their sponsoring institutions, in those same journals, as a databank of refuseniks and frauds.

o Prohibition of the use of computer models in public policymaking (as in sworn testimony before Congress) that have not been certified, or audited, much as financial statements of publicly traded companies must now be audited.

o Licensing by the state of sale and conveyance of computer models of general economic or social significance, perhaps as defined and maintained by the National Academy of Sciences.

The last is extreme, of course, implying enormous bureaucracy and infrastructure to accomplish, and probably itself inevitably subject to abuse. The reforms are all distasteful in a free society. But if we do nothing to put our house in order, much worse is likely to come from the pen or word-processor of a technically naive legislator.

In exchange for a profession's privileged status, society demands it be self-policing. Doctors, lawyers, CPAs and the like are expected to discipline their membership and reform their methods when (preferably before) there are gross abuses. Although some of them have failed to do so in recent years, is that an excuse for us not to?

Finally, how can we ensure that McNees' prediction, that people will continue to re-engineer our society on models no better than garbage, will prove as false as the models he has described?

Search RISKS using swish-e

THE RISKS DIGEST

Forum on Risks to the Public in Computers and Related Systems

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

Volume 4: Issue 22

Tuesday, 2 December 1986

Contents

More Air Traffic Control Near-Collisions

Peter G. Neumann <Neumann@CSL.SRI.COM>
Tue 2 Dec 86 10:08:05-PST

Chicago (UPI) 2 Dec 1986

Two passenger jetliners on their landing approaches nearly collided with small planes in separate incidents here yesterday, the Federal Aviation Administration said. The near-collisions, which occurred within 29 minutes of each other, involved a Midway Airlines DC-9 with 90 people aboard, arriving from Philadelphia, and a United Airlines Boeing 727 with 128 people, en route from Baltimore. FAA spokesman Mort Edelstein said that the United pilot reported passing within 500 feet laterally of a twin-engine Beechcraft

> 90 about 28 miles southeast of O'Hare International Airport at 7:41 a.m.
> The pilot made a sharp left turn to avoid the smaller aircraft, he said.
> According to Edelstein, a preliminary inquiry found that the smaller plane
> had a defective transponder that was transmitting inaccurate data on the
> plane's altitude to air traffic controllers in Aurora, west of Chicago.
>
> [The second incident was less close, and no explanation was given.]

The problem of an accidentally malfunctioning transponder is in many ways equivalent to that of an intentionally malfunctioning transponder -- either one that has been purposely sabotaged in an attempt to jeopardize the plane or one that has been altered "constructively" in an attempt to hide the true altitude of the plane. In all of these cases, the ATC system implicitly trusts the authenticity and accuracy of the transponders with which it communicates -- if such a transponder exists at all in a private plane.

Re: satellite interference

Jerome H. Saltzer <Saltzer@ATHENA.MIT.EDU>
Mon, 1 Dec 86 23:37:50 EST

About a month ago, Richard Wexelblat reported to RISKS that satellite delivery of the Headline News Network to his location was disrupted for a short time by an interfering signal whose picture wasn't intelligible but whose sound seemed to be advertising satellite decoders. In contrast with the Captain Midnight attack on HBO, no big follow-up story appeared in Newsweek and Time magazines.

My contact at the F.C.C. tells me that there are typically a couple of incidents like this every day. The primary problem is not malicious attacks by a Captain Midnight. It is simple screwups by uplink operators who forget to throw switches, who set wrong channel numbers in their transmitters, who aim their dishes at the wrong satellite, or who run automatically programmed switching sequences that were intended for yesterday or tomorrow rather than today.

The reported audio content sounds suspicious, but it turns out that a scrambled video service usually has an unscrambled audio channel accompanying it that explains how to obtain a decoder and subscribe to the service. The audio that goes with the picture is buried somewhere else in the channel.

F.C.C. technicians have proposed to tackle the operator screwup problem by requiring that uplink transmitters place encoded call letters in the vertical retrace interval of their transmitted waveforms. Then at least someone who is being interfered with can quickly figure out which of the 1200 licensed uplink transmitters is muddled up and get the operator there on the phone quickly. That solution doesn't eliminate intentional attacks by someone who knows how to forge the unique id, but from the F.C.C.'s point of view it will solve 99.9% of the problem they face. As for malicious cases, detective work and $10,000 fines may help keep things under control.

Although the technology is different, don't the problem and the proposed

solution both sound quite familiar to the regular reader of RISKS?

Jerry

"Welcome to the ..... system": An invitation?

Bruce N. Baker <BNBaker@SRI-STRIPE.ARPA>
Tue 2 Dec 86 10:35:05-PST

At a local chapter meeting of the Information Systems Security Association, a representative of VM Software Inc. told a story about a Massachusetts financial institution that had attempted to prosecute a hacker who had penetrated their system. The defense lawyer argued that the system had a greeting that welcomed people to the system and that was tantamount to welcoming someone into your home (Goodbye, Welcome mats?).

The judge threw out the case accepting the arguments of the defense.

I have attempted to track down the authenticity of the story through the VM Software rep but he will not divulge the name of the company.

Attempts to track it down through the law firm of Gaston Snow & Ely Bartlett in Boston revealed no records of such a case.

Obviously, if there was such a case it has implications to the wording of the Welcome banner on any system.

Can anyone provide a better lead or lend credence to the story?

Replicability; econometrics (Re: RISKS-4.21)

Charles Hedrick <hedrick@topaz.rutgers.edu>
Mon, 1 Dec 86 12:13:24 est

I have had a long-term concern with replicability of scientific experiments. It does not appear that this concern is shared outside of certain physical sciences. When I was a grad student, I published an article in the American Economic Review (the economic equivalent of CACM). In order to allow replicability, I included the actual data, together with the details on how I had adjusted the raw data series (something which has to be done because the agencies change definitions every few years). The data was small compared to the size of the article. It was cut for space reasons. My article itself was a replication of an empirical study done some years ago. It covered a period when the economy had behaved very differently. It came to the same conclusions. The original study had been very careful about econometric validity. It is possible to do valid work in econometrics. It is also possible to duplicate carefully done work. [I think these comments are important because they show that econometrics is not necessarily voodoo. What we need are professional standards to help us separate the good work from the bad.]

Similar problems occur in computer science. Several years ago, one of our grad students attempted to duplicate the results of researchers in one area of AI. He was trying to do research into what actually causes success in rule-based systems. He ran into serious problems with another research group, which went beyond simply refusing to give data. I think our department would prefer for me not to give any more details. But he concluded that such work was impossible in the particular area with which he was involved.

In my opinion, anyone who publishes empirical claims in a scientific journal should be required to give people access to the data needed to replicate it or do further analysis of its model. I have been unable figure out what to do to try to make that happen.

By the way, I have a related Risk to describe. As I mentioned above, in econometrics one normally has to twiddle with the basic data series in order to get useful numbers. I am now a computing manager. I find that our users expect to have access to various commercially-prepared econometric data series. As far as I can see, all that is there is a bunch of numbers and a one-line description of what it is. When I was doing work in the area, I would have wanted to know a lot more about how the numbers had been prepared. I'm hoping there is some sort of hardcopy document available to users of the databases, but I'd bet even if there is, a lot of our users never see it.

Re: Risks of computer modeling

John Gilmore <hoptoad!gnu@lll-crg.ARPA>
Tue, 2 Dec 86 05:39:29 PST

> Is the problem restricted to econometrics, or is the abuse of computer
> modeling widespread?

It is widespread.

One friend of mine has done extensive work in "decision analysis" systems, with clients in the military, Bell System, etc. I did some programming on such a system for him while he was at SRI. When looked at from the inside, it is obvious that such a system will give you back exactly the answers that you fed it as input, since most of the input data is "How important is this? How important is that?". But people will believe it because a computer model said so, while if *you* told them that the widget acceptance ratio was 33% if priced at this level, they would ask you why. They didn't get to ask when you typed it in.

Another friend works for the World Bank in Washington, DC. She has done a lot of proposals and evaluations around funding of transportation projects in third world countries. I remember helping her get some of her modeling programs right. Her approach was always to figure out what the data "means", in other words, what result she wanted, and then juggle the numbers and equations until she could "prove" it.

I don't think that abuse of modeling is restricted to computer models, or even that it is more prevalent with computer models. In all disciplines,

experienced people with a feel for things figure out what is going on and proceed from there. If somebody wants better justification, they have to cook one up, but don't mistake the source of the estimate: the human mind, not the later model.

Cf. ``How to Lie with Figures''. Don't have the citation but it's a standard work. Maybe it needs an update to deal with new techniques.

Computerized weather models

Amos Shapir <nsc!nsta!instable.ether!amos@decwrl.DEC.COM>
1 Dec 86 10:02:31 GMT

About weather models: they are one of the few accurate forecasting models possible; the only trouble is that the required answers, e.g. 'will it rain on the game tomorrow?' are much more detailed than the base data (typically a 3-6 hourly surface report from stations 50 miles apart). Besides, until Crays came along, it was almost impossible to do it in real time.

Amos Shapir, National Semiconductor (Israel)
6 Maskit st. P.O.B. 3007, Herzlia 46104, Israel
(011-972) 52-522261 amos%nsta@nsc 34.48'E 32.10'N

Active control of skyscrapers

Warwick Bolam <munnari!goanna.oz!wjb@seismo.CSS.GOV>
Mon, 1 Dec 86 14:05:28 EST

> Date: Wed, 26 Nov 86 13:32:05 EST
> From: "Kim P. Collins" <kpc%duke.csnet@RELAY.CS.NET>
> To: RISKS@CSL.SRI.COM
> Subject: Very Brief Comments on the Current Issues
>
> New subject
> Any comments on active vs. passive control structures? For instance,
> having a skyscraper that has flexible material so that in high winds
> it bends and does not fail, VS having a skyscraper that has guy wires
> connected to winches that are controlled by a computer that tests wind
> velocities, etc.

There already exist active control systems for skyscrapers that use a huge mass, that is "pushed around" by computer controlled equipment to stabilise the building. I'm afraid I have no reference to this. I saw it on TV.

Warwick Bolam

UUCP: seismo!munnari!goanna.oz!wjb ARPA: munnari!goanna.oz!wjb@SEISMO.ARPA

Privacy in the office

Paul Czarnecki <harvard!munsell!pac@seismo.CSS.GOV>
2 Dec 86 16:19:49 GMT

There is an interesting article in the November/December 1986 issue of Technology Review that I though may be of interest to RISKS readers. The title is "Monitoring on the Job: How to Protect Privacy as Well as Property." The authors are Gary T. Marx and Sanford Sherizen.

The article discusses how surveillance technology is used in the modern office environment. Everything from video cameras in the parking lot to private data on corporate machines is discussed. Although much of the technology is not computer related, some of it is.

I thought the article was interesting overview of some of the issues involved with technology and privacy. It was not as in-depth as I would have liked, but good anyhow.

pZ

Paul Czarnecki -- Eikonix, Corp. -- Bedford, MA
{{harvard,ll-xn}!adelie,{decvax,allegra,talcott}!encore}!munsell!pz

---

!!! Kremlin is purging dimwitted scientists !!!

M P Wiener <weemba@brahms.berkeley.edu>
Mon, 1 Dec 86 01:31:38 PST

The following is shamelessly stolen from the 2 Dec 1986 edition of the WEEKLY WORLD NEWS. (You couldn't have missed that issue while shopping: it had the banner headlines about the five-week long pregnancy [Bulgarian natch] and a recipe for cooking Thanksgiving turkeys in the dishwasher.)

- -

<< Lame-brained Russians try to fix computer -- with a hammer <>

!!! Kremlin is purging dimwitted scientists !!!

Soviet official launched a massive investigation into the training of technical personnel after a repairman tried to fix a sophisticated missile guidance system with a hammer, a screwdriver and an oil can.

A recent East German defector, Dr. Hermann Franz, blew the lid off the shameful state of Soviet technical know-how in a scathing letter to top science journals upon his arrival in the West.

The computer scientist, who is now living in France, claims there is a very real danger that a poorly-trained Russian technician might accidently start World War 3.

``The repairman with the oil can is a glaring example of their in-eptitude,'' said the expert. ``He was assigned to one of the most sensitive missile bases in the U.S.S.R.

``And yet, when he was called on to repair a circuit problem in a computer console, he showed up with carpenter's tools.

``First he walked over and kicked it. Then he said, `Something is

stuck.' I thought he was joking until he started squirting oil and blew every circuit in the control center.

``It took six weeks to repair the damage -- six weeks to do a job that qualified technicians could have done in a matter of days.''

Horrifyingly, the missile base near the foot of Ural Mountains is armed with some of the Soviet Union's most powerful intercontinental missiles and nuclear warheads, Dr. Franz said.

A Soviet Air Force spokesman angrily denied the allegations, calling Soviet technicians ``the finest in the world.''

One highly-placed military source conceded that Soviet training programs are being investigated. But he insisted that the investigation was routine.

Meanwhile, Dr. Franz has called on Western politicians and scientists to pressure the Soviets into monitoring the work of their technicians more closely.

``The specter of nuclear holocaust is frightening enough,'' he said, ``without having to worry about some dimwit starting the war that would kill us all.''

-- Derek Clontz

- -

I don't quite follow the logic of that last quotation. Personally I'm more worried about some of the "dimwits" at the other end of the nuclear chain of command.

I have two questions:

Q1) Can anyone identify a quote top science journal unquote that is publishing Dr Franz' letter? (Heck, while we're on a roll, can anyone confirm the "Clark Gable's our god, says lost island tribe" story?)

Q2) What is known/believed about Soviet failsafe mechanisms?

ucbvax!brahms!weemba Matthew P Wiener/UCB Math Dept/Berkeley CA 94720

Search RISKS using swish-e

THE RISKS DIGEST

Forum on Risks to the Public in Computers and Related Systems

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

Volume 4: Issue 23

Wednesday, 3 December 1986

Contents

The persistence of memory [and customs officials]

Richard V. Clayton <clayton@bambi.bellcore.com>
Wed, 3 Dec 86 07:27:13 est

The 27 November issue of New Scientist has an article (page 20) about a heroin smuggling ring convicted with the help of evidence obtained from a pocket computer. The smugglers used the computer, a Psion Organizer, to store information about deals; after the deal was done, the information was erased. However, the Organizer uses EPROM storage, so information wasn't erased, but flagged as being unavailable. After seizing the computer, customs officials took it to Psion where in-house software recovered the information.

America's Cup - floppies held to ransom

<derek%gucis.oz@RELAY.CS.NET>
03 Dec 86 18:30:18 +1000 (Wed)

I thought RISK readers might be interested in some of the lighter risks associated with the use of high technology in twelve metre yachting. Not only must keels be covered!

CUP INFO RANSOMED (From Computing Australia, 1 December 1981)

A stolen package of floppy disks holding sensitive telemetry data from one of the America's Cup syndicates has been recovered after being held to ransom through a hacker's bulletin board.

The theft of the 17 disks came to light on a bulletin board called Inter-State Connect, where a note was posted originally asking $10,000 for them.

It is not known which syndicate had the disks stolen as no name appeared on them and none of the yachting teams have admitted ownership.

The disks were stolen in Fremantle and turned up in Melbourne where computer security analyst, Stuart Gill, negotiated the retrieval of the disks through a shadowy organisation of hackers known as TechHack.

TechHack became involved in the negotiations after being accused of mounting the ransom operation. In order to clear its name, TechHack acted as the intermediary between Gill and the hacker responsible for the ransom notice.

Computing Australia has obtained a printout of the negotiations which took place on the bulletin board.

It reads:

> As at 21/10 we require the sum of $2,500 for the exchange of the disks Confirm there are 17 and you are aware from our Perth contact that they are Kosher. We cannot continue talking for much longer as we don't think you are serious.

In the end, the stolen property was retrieved with no exchange of money.

It is believed a number of syndicates approached Gill for copies on the disks on the pretext of establishing where they came from.

<end-of-article>

Some thoughts regarding recent postings: blame and causality

Eugene Miya <eugene@AMES-NAS.ARPA>
Wed, 3 Dec 86 10:13:07 pst

Peter, your recent note on the frequent but rarely discussed topic of "where

to place the blame" concerns me. It seems that we in computers and computer science have some what ill-defined concepts of CAUSALITY (where DO we put the blame?), (non)determinism, and our poor use of reductionism. Other similar postings on modeling and empirical data as final proof also concern me.

Consider, the mistake we make when we confuse WORK and EFFORT: we get Brooks' mythical man-month. (Brooks' classic example was 1 woman => 1 baby in 9 months, therefore 9 women => 1 baby in 1 month.) And there are many people who don't see that this generalizes in high-performance computing in terms of mythical MFLOPS: some programs are not decomposible into parallel parts. And I suspect this is also manifest in the way we use redundancy in fault-tolerant computing (multiple CPUs in hot-start configuration which could be used for parallel computation but are used for reliability instead).

I think we misunderstand causality for two reasons:

1) Our empirical foundations tend to be a bit weak. (We put theory quite high in esteem.) In part, mathematical theory is our solution, but it also a source of bias. I know many will disagree with this latter conclusion including PJD. We try to envision problems outside of the complexities of the `real' world (modeling and simulation). Where as theoretical physics had experimental physics to fall back on, computer science does not have a good equivalent.

2) Some of our ideas do not tend to generalize across computers as mathematical concepts generalize across the mathematical sciences. We are not really JUST a mathematical science. The recent econometric postings enforce some of this.

I heard an interesting thing about the way computing is done in third-world countries (I heard the USSR was/is in this category) where computing is expensive and thinking is cheap:

Theoretical CS is held is high esteem because when a mistake is made in hardware or in a project it becomes glaringly visible to all. When mistakes are made in theoretical CS (and probably math to a lesser degree), there are so few people who understand these ideas, and some ideas are so specific, that only a few people can criticise them (fewer/less negative reinforcement and punishment).

Consider the discussion on testing: computer people talk about testing with respect to the correctness of a specification, but we don't talk about testing with respect to the `real' world. Testing of accounting programs is one thing, but testing of models of the physical world like fluid dynamics or population quality of life are different things. Perhaps I should use the word measurement here. There are numerous cute computer models with graphics like the LLNL crushed cone shown at the 1984 SIGGRAPH or similar fluid dynamics works here. (References provided on request.) I fear that we computer types have a greater chance of losing touch with reality. This would also make us among the poorest judges in our own discipline for things such as the Turing Test because the Test is ultimately an empirical endeavour.

Anyway, these are some initial thoughts I have composed over the past few

days about computing's poor basis in empiricism.

--eugene miya

Microcomputer controlled cars (not Audi)

Controls Wizard <dma%euler.Berkeley.EDU@berkeley.edu>
Wed, 3 Dec 86 08:23:12 PST

There's been a lot of discussion about the Audi problems and I remembered a similar incident. The Sept. 1984 issue of Consumer Reports included a review of the Mitsubishi Starion. Under the heading "Defect of the Month" they described uncontrollable acceleration that was only stoppable by turning off the ignition. The problem was eventually solved by replacing the engine microprocessor and the problem was reported to the National Highway Traffic Safety Administration. It seems to me that NHTSA should be getting the Audi complaints and telling Audi that they should look at the source of the problem. Precedents are a good way of convincing people that there's a problem. Miriam Nadel

Re: Welcome to the system

<Henning@DOCKMASTER.ARPA>
Wed, 3 Dec 86 10:59 EST

I know of a similar case that never made it to court. The computer security administrator at Roche, the drug company had been plagued by a hacker who auto-dialed the entire Roche phone system in sequence. It took a lot of phone calls from company management to convince the phone company that this was not just someone with fast fingers and a touch-tone phone. They laid a hacker trap on one of the PC`s and traced the call. Once the suspect was found, it was even harder to get him arrested since he was in New York and Roche is in New Jersey, which somehow got the FBI involved.

The perpetrator was brought into the police station and had the riot act and the fear of God scared into him. He was not charged -- because there wasn't a no trespassing sign on the hacker trap identifying the system as private property of Roche.

> [A tough Roche to phone? (All Roche leads to phone?)
> Yes, this has been a common problem in the past... PGN]

Re: Automated trading

Scott Dorsey <kludge%gitpyr%gatech.csnet@RELAY.CS.NET>
Sun, 30 Nov 86 14:04:18 est

I'm afraid to say that most of the programs all use very similar algorithms with almost identical buy/sell setpoints. That's where

the problem probably lies.
The solution is to predict the changes in the market that would result from these (very predictable) programs operating at the same time, and I am sure that some smart fellow will be making a lot of money that way...

Active control of skyscrapers

<LIN@XX.LCS.MIT.EDU>
Wed, 3 Dec 1986 09:20 EST

[...]
I'm told that the John Hancock Building in Boston is built like this.

Sanity in Automating Keyword Abstracting

Paul Ryan <dgis!ryan@lll-tis-b.ARPA>
Mon Dec 1 16:30:30 1986

The Defense Technical Information Center (DTIC) acts as the central repository of scientific and technical information for the Department of Defense (DoD). One of the four online databases which DTIC maintains is the Technical Reports Database. It has recently come to our attention that the 29 September 1986 issue of the RISKS Digest [RISKS-3.70] was informed of a "new policy" by DTIC that stated that technical report titles be designed with keywords positioned in the first five words of the title. THIS IS NOT AND NEVER HAS BEEN A POLICY OF THE DEFENSE TECHNICAL INFORMATION CENTER. Apparently, this erroneous information was forwarded to this forum as an example of the risk to accurate dissemination of information caused by faulty programming (or programmers?).

The policy of this organization regarding technical report titles is that they should reflect the author's effort to describe the content of the report.

In trying to determine from where such an inaccurate statement might have developed, our conclusion is that the individual (outside this organization) who proposed the "policy statement" misapplied a long standing DTIC search retrieval capability. Our automated retrieval system has a search algorithm which is constructed from the first five words of the title. It allows a searcher to identify a report title and bibliographic citation from our online collection of 1.5 million titles. The search retrieval algorithm works for any word of the first five words of the title whether they be prepositions, articles, or keywords in identifying the bibliographic citation associated with a title.

For further information please contact: R Paul Ryan, Director, Office of User Services, Defense Technical Information Center, Cameron Station, Alexandria, VA 22304 Phone (202) 274-6434 AV 284-6434

Search RISKS using swish-e

Report problems with the web pages to the maintainer

Search RISKS using swish-e

THE RISKS DIGEST

Forum on Risks to the Public in Computers and Related Systems

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

Volume 4: Issue 24

Friday, 5 December 1986

Contents

Criminal Encryption & Long Term effects

<baxter@ICSD.UCI.EDU>
Thu, 04 Dec 86 17:54:14 -0800

In a previous RISKS article, mention was made of a prostitution ring that used computers to keep track of the customer base. It was only moderately surprising that "criminal elements" would finally arrive at a use for data processing technology (as opposed to victimizing it...). Having built file systems which automatically decrypt records when accessed (for password storage, etc.), I have long been surprised that the use of encryption as a technique for storing such transactions has not received widespread use, or that at least a spectacular instance has not been uncovered. For a bookie, surely the convenience of pulling the plug on a computer during a police raid and taking the 5th when asked for an encryption key must outweigh the difficulty of handling and destroying flimsy tissues (no, I'm not sure what

technology bookies actually use). The first conclusion is that computing (and technology supporting privacy) may make a life of crime more convenient and safer, raising the spectre of a permanently entrenched criminal computing element.

A more chilling thought is perhaps the long term consequence of police reaction to this: acquisition of privacy-breaking technology, and use of such technology to detect criminal transactions before arrests occur.

Criminals and encryption

Phil Karn <karn@ka9q.ampr.net>
Fri, 5 Dec 86 03:17:51 EST

I am interested in documented criminal cases where defendants have encrypted their communications or incriminating computer files and refused to divulge the keys under their Fifth Amendment rights. I am particularly interested in the response of the legal system in such cases and the effect, if any, encryption technology might have had on the outcome. I can think of many possible scenarios, such as:

1. The police either trick the defendent into revealing the key, or by exploiting his carelessness (by finding it written down or easily guessed, etc) recover the information which is then used in the prosecution.

2. When more than one person knows the key, one is given immunity and compelled to divulge it to produce evidence against the other(s).

3. The police perform a successful cryptanalysis.

4. The police and prosecution are unable to recover the encrypted information, but obtain a conviction anyway in the traditional way (through witnesses, physical evidence, etc).

5. Without the encrypted information, the case is dropped due to lack of evidence.

Much of the evidence in certain types of criminal cases consists of paper records and intercepted telephone conversations obtained through warrants. (Political corruption, drug rings and organized crime come to mind). I am interested in the issue of how the widespread availability of computers and encryption devices will affect the criminal justice system. Clearly, it will be impossible to keep this technology out of the hands of criminals (at least in the US). Will prosecutors find other, equally successful ways to get convictions? Or will there be mounting pressure to erode Constitutional due-process guarantees and the right against self-incrimination? Even worse, will there be misguided and futile attempts (along the lines of the Electronic Communications Privacy Act) to control the availability of computers within the United States in the name of "law and order" or "national security"?

Phil

Re: ATC Near-Collisions

Rony Shapiro <ronys%wisdom.bitnet@jade.berkeley.edu>
Thu, 4 Dec 86 11:13:19 -0200

I would like to comment on the article from Chicago (UPI) Dec 2 1986.

The fact that the transponder on the light aircraft was defective may be misleading. Air-traffic controllers are trained (at least here) NEVER to rely on tranponder altitude reports when assigning altitudes to other aircraft. In other words, the controller appeared to have erred in trusting the transponder when giving the jet clearance to land.

Transponders are not perfect, & their transmissions may get garbled, especially in a crowded airspace, such as Chicago. However, as long as they are regarded as such, they are a useful aid in air traffic controlling.

Trusting transponders too much is a great temptation under heavy workloads (easier than asking the pilot of the aircraft in question his altitude - the only sure method), but the blame is with the ATC, & not with the transponder.

Rony Shapiro. <ronys@wisdom>

High Availability Systems

Peter G. Neumann <Neumann@CSL.SRI.COM>
Thu 4 Dec 86 09:30:22-PST

There is an ad in the 4 Dec 86's SF Chron for "California's most convenient ATMs". The banner across a depicted terminal screen says "NOW 24 HOURS A DAY" (implying that until recently it wasn't?). The text of the ad says "VERSATELLER ATMs are there ... when you need them ... With 24-hour service all day and all night.*" (as opposed to 24-hour service just during the day?) The footnote in VERY fine print says "* Available at most locations and subject to routine system maintenance 2 a.m. to 6 a.m. Sumday."

[There was a time when ATMs would run stand-alone when the central computer was down, but there were some cases of people grossly exceeding limits intentionally during such times. Is this no longer the case? The Airline reservation systems also have the maintenance problem of having to shut down, but that is presumably because of large numbers of schedule changes that for some peculiar reason cannot be queued up dynamically and cut over at a particular time. There are lots of interesting risks associated with upgrading and/or maintaining more time-critical systems that cannot afford to be down at all... PGN]

Plug-compatible modules

Peter G. Neumann <Neumann@CSL.SRI.COM>
Thu 4 Dec 86 09:36:38-PST

The 4 Dec 86 SF Chron has an AP story on a 4-year old girl who was electrocuted when a nurse accidentally plugged her heart-monitoring line into an electrical circuit. (Children's Hospital, Seattle WA) Using a standard male electrical plug on such a line seems incredible. I mention it here as a generalized example of the lack of strong typing (type safety). Compatibility among different types is a common and serious problem in computer programming languages and system calls, but this case is somehow amazing...

"Satellite interference" (CNN Headline News)

Lauren Weinstein <vortex!lauren@rand-unix.ARPA>
Wed, 3-Dec-86 12:33:42 PST

While misaimings and such are fairly common, they rarely result in total capture of a satellite transponder, since it takes considerable power to completely override the main signal. In the case of the described problem with CNN Headline News, the explanation is almost certainly very simple and has nothing whatever to do with interfering signals.

Both CNN services (as are a variety of other satellite services) are scrambled with the VideoCipher II system (designed by MA/COM, now owned by General Instruments). The system uses DES technology and has the capability of an in-the-clear "barker" audio channel that promotes the service and (in the case of CNN) the sale of decoders as well. The VC II technology is very sensitive to signal levels and quality--if the level drops off or glitches momentarily the unit will fall back into its "deaddressed" mode and send the encrypted video and the audible barker to the output (in most cases a cable system). It can take anywhere from a second or two to many minutes (sometimes hours under poor conditions) for the VC II to resync and restore normal output.

The case described almost certainly was a VC II dropout at the local cable company that resulted in the encrypted picture and clear barker being sent to the cable system subscribers.

By the way, the proposal the FCC has made about ID's in the vertical interval will not sit well with many programmers--the vertical interval is sometimes used for other purposes (teletext, audio services, etc.) and those programmers can be expected to vigorously object to "wasting" their interval on a visible I.D. Of course, if only "occasional" uplinkers (such as remote news crews) were required to do this, it would not be such a problem since such crews virtually never are sending any special vertical interval information.

--Lauren--

Re: Privacy in the office

Brint Cooper <abc@BRL.ARPA>
Wed, 3 Dec 86 23:13:16 EST

All offices are not equivalent. In components of the DoD, as we are made painfully aware, "Use of official telephones implies consent to monitoring." How "they" monitor, whether computers are used, and how the monitored content is validated, are anyone's guess.

Brint

ACARD Report

Samuel B. Bassett <well!samlb@lll-crg.ARPA>
Wed, 3 Dec 86 23:35:11 pst

In regard to the ACARD report, it strikes me that what the British commission is trying to do is to force businesses and organizations to accept the idea of product liability in an increasingly critical area. The British system allows the sort of "persuasion from on high" that we in the U.S. would never put up with. (Can you imagine how much money would be available to a PAC to _defeat_ the first Congresscritter to introduce such a bill here?)

It may be that this is a political "stalking horse" -- an early attempt to put the idea in the public domain, let it get argued over for a few years, and avoid a direct political battle in the near future. The wording has that peculiar British Civil Servant flavor to it, which indicates to me that it is mostly a thoeretical exercise at the moment.

In any event, serious programmers and software engineers should welcome the news of the report -- it will strengthen their hands when talking to management about realistic time scales for software projects. The literature has been full of breast-beating about how good software would be if management didn't persist in rushing it out the door without proper testing? Now they have a good arguement to hit 'em with.

Then too, in the last analysis, even if the report were enacted into law, it is doubtful if many (or any) programmers would go to jail -- but it would be almost certain that more than a few companies would lose a _lot_ of money. Managers pay attention to such things . . .

Sam'l Bassett, Self-Employed Writer
34 Oakland Ave., San Anselmo CA 94960;
DDD: (415) 454-7282; / dual\
UUCP: {...known world...}! lll-crg!well!samlb;
Compuserve: 71735,1776; \hplabs/

Report problems with the web pages to the maintainer

Search RISKS using swish-e

THE RISKS DIGEST

Forum on Risks to the Public in Computers and Related Systems

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

Volume 4: Issue 25

Sunday, 7 December 1986

Contents

Child electrocuted (RISKS-4.24) (anonymous contribution)

<NEUMANN@CSL.SRI.COM>
Fri, 5 Dec 86 17:19 PST

This contribution was sent to me privately, but is being distributed anonymously -- at my request -- with the permission of the author.

> I used to volunteer in the Emergency Room at a SF hospital, and the heart monitoring lines there had about six pins arranged in a circle, similar to the bottom of vacuum tubes. The exposed pins were shielded by a heavy (1/8-in thick) metal ring with a key which permitted it to be plugged into the proper receptacle in only one orientation. Every EKG line I've ever seen (including some at other locations) is compatible with this configuration.
>
> Unless someone had built a non-standard connector for this particular

monitor line, such an electrocution would not have been possible with a standard electrical receptacle. [...]

Child electrocuted

Brad Davis <b-davis%utah-cai@utah-cs.arpa>
Fri, 5 Dec 86 18:42:50 mst

If this is true then I don't think that the equipment met Underwriter Lab's (UL) safety specs. They have some strict requirements on what certain plug designs can be used for and how current carrying plugs can be configured.

Brad Davis {ihnp4, decvax, seismo}!utah-cs!b-davis b-davis@utah-cs.ARPA

Child electrocuted

<ssc-vax!ssc-bee!nelson@beaver.cs.washington.edu>
Fri, 5 Dec 86 15:30:32 pst

[...] The leads were incorrectly inserted into the end of a power cord for an IV pump, causing the electrocution. This particular IV pump had a detachable power cord for portable battery-powered operation. Most all news reports that I have heard put the blame on human error (Nurse electrocutes child patient...).

How this could happen was beyond my comprehension until I watched the news and had a look at the ends of the power cord for the IV pump and the cord for the heart-monitor equipment. The ends were very similar in shape and the heart-monitor leads actually fit into either [termination] without much difficulty.

Besides the obvious finger-pointing consequences of this incident, I was immediately hit with the grave psychological damage that must have been caused to both the nurse and child's family. The ultimate risk of living in our "high tech" society had certainly been realized by them.

Paul Nelson, Boeing Aerospace Co.

On models, publications, and credibility

"ESTELL ROBERT G" <estell@nwc-143b.ARPA>
5 Dec 86 11:21:00 PST

Perhaps one way to encourage researchers and authors to take more care with their data and their models would be for some leading journals [e.g., ACM and IEEE pubs, among others] to encourage authors to submit complete listings of programs, and data, in appendices to papers. For lack of page space, many such appendices would NOT be printed with the articles. But the information could be made available from

the publisher, via network, or floppy disks, for a reasonable fee.

Some work will involve sensitive data, or proprietary models. In such cases, sometimes the data can be "sanitized" and sometimes the model can be described generically. That won't be a lot different from today's situation, where models and data rarely appear in detail.

On the subject of "getting the right(?) answer" we need to remember [and tell our non-computing colleagues] that even the "facts" that we seek as data influence the decision; ditto the model design, and the parameterization of the model. One of my grad school profs told a story of working for Getty Oil: J. Paul's two sons [half brothers] were rivals; one had North American operations; the other, European. The European leader proposed some corporate scheme; my prof's assignment was to "prove him wrong." So they went to work on a model; fed it some good estimates; and it agreed with the European recommendation; modified the parameters, and re-computed. ... On the 253rd such iteration, the model finally said that the brother was wrong. It was that last case that the USA manager took to his dad, who believed it.

That doesn't necessarily mean they cheated. How many models of the DNA structure were wrong, before the right one was found? How many bad airplane designs crashed, before Kittyhawk? How many flawed page replacement algorithms, or sort algorithms, et al, have we tried? For the candy maker, good "fudging" is obviously progress; the rest of us have to wonder.

The power of computer models is that they allow us to try out so many ideas, or variations of them, so rapidly, so inexpensively. The risk of computer models is that we accept their results, without critique. I contend that tinkering with a model and its data are proper; and that the results of the Nth iteration may well be better than the results of the "first best guess." But the reasons for believing any model output must rest on a *causal link to reality.*

Bob

Encryption and criminals

Perry Metzger <metzger@heathcliff.columbia.edu>
Fri, 5 Dec 86 19:02:23 EST

One of the classic books on this subject, "The Code Breakers" by Kahn, discusses the incidents during prohibition with rumrunners and encryption. It seems that earlier in the century commercial codes were widely used.

One of the more humourous incidents listed (reminiscent of trials involving technology today) was during the trial of one set of smugglers in which a star witness was a cryptanalyst who was quite incompetently questioned by the defense. The lawyer's ignorance of the techniques used was hysterical, and reminiscent of what happens today.

But back to the subject, during prohibition the law enforcement

agencies would quite often call in outside help and try to break the codes involved, often with success. So far as I could tell from the book, this did not lead to wide-scale abuses of any sort involving the police trying to crack commercially used codes and the like.

After all, breaking a code is a long and labour intensive task. You don't do it unless you have to. Routine breaking of encryption by the police will not be a reality any time soon.

Perry Metzger

[Although in a real crunch, there are skilled cryptoanalysts around who could probably be brought into the fray.]

Encryption and criminals

"Fred Hapgood" <SIDNEY.G.HAPGOOD%OZ.AI.MIT.EDU@XX.LCS.MIT.EDU>
Sun 7 Dec 86 07:40:35-EST

Re encryption by criminals. Some years ago I fell into conversation with a gentleman who worked as an IRS prosecutor. Occasionally he brought a house of prostitution before the bar, and they routinely encrypt their client lists and financial records, and probably have for millenia.

He had no interest in spending the time trying to break their codes. What he did was subpoena the records from their towel company, multiply the number of towels they used by the average charge, and bill them for the tax due on that amount. He said the Courts proved happy to accept that document.

Mode-C altitude transponders

Dan Melson <crash!dm@pnet01>
Sat, 6 Dec 86 17:14:35 PST

ronys@wisdom writes "ATC is trained to never trust a transponder"

I'm sorry, but this is incorrect information. ATC is trained to verify, at the time the pilot checks on frequency, that the mode-C is accurate. If, of course, the pilot is not talking to the controller, there is no way for that controller to know that mode-C is verified.

Phraseology for issuing traffic on unverified mode-C readouts includes telling the pilot that we have no confirming report that mode C is correct.

However, a verified mode-C readout *is* used as basis for separation.

DM

ATM Limits

Richard Outerbridge <outer%csri.toronto.edu@RELAY.CS.NET>
Sat, 6 Dec 86 07:44:10 est

Typically ATMs are hung off a controller, which acts as a front-end for the bank's mainframe host. The controller often performs a lot of the normal processing anyway - for instance, pin verification and sanity checking - and can usually "stand-in" for the host while the latter is down. One mechanism used to prevent fraud is a "cycle file". This keeps a record of all the cards used within a 24-hour period along with the amount of cash dispensed to each. The "cycle limit" is either pre-defined (according to the "type" of card) or read from the card itself. So, if the host is down, you may be able to withdraw up to your daily "cycle" limit at 23:55 and again at 00:05, but only every two days. If the cycle limit is recorded on the card, by re-writing that field you may also be able to withdraw virtually unlimited amounts of cash (again, if the host is offline).

If the controller is down, the ATMs will be closed, but usually the controller is more stable than the host. In the event of hardware failure the only solution is a "hot" backup controller which can be switched over to resume processing, albeit after a brief interruption of service. If more than one controller is attached to the host, then each will maintain its own cycle file; if you knew the network you could withdraw your cycle limit from each.

Taking the 5th

<LEICHTER-JERRY@YALE.ARPA>
6 DEC 1986 10:35:22 EST

I asked a lawyer friend about this issue - a criminal with encrypted records refusing to divulge the key, citing the fifth amendment - a couple of years back. His strong feeling - and, of course, until someone actually pushes such a case, probably to the Supreme Court, all you can GET are feelings - was that there was no way a court would uphold such a claim. The Fifth Amendment lets you refuse to provide information ABOUT possibly-criminal activities. It does NOT allow you to avoid turning over evidence. In general, the courts guard their rights to obtain evidence very jealously, and interpret limitations on those rights as narrowly as they possibly can. (Consider the various "shield laws" that states have passed to allow journalists to protect their sources. Even with fairly explicit laws on the books, courts, when they've found a need for journalists' testimony, have found ways to force it.)

In practice, I doubt it makes much difference. The worst that is likely to happen to you for refusing to testify is a couple of months in jail. (There are typically two stages: The court first jails you "until you reconsider your refusal". In principle, this can be forever. In practice, when it becomes clear that you will not change your mind, we move to a second stage, where you may or may not be held in contempt of court. I don't know what the maximum sentence for contempt is, but typical contempt sentences seem to be a couple of months.) So a real criminal is likely to see this as an excellent trade-off.

This whole issue, BTW, illustrates an interesting point. Those of us who are heavily involved with computers, networks, and so on, as technologists, tend to see what we do as entirely new and unprecedented. Lawyers tend to view EVERYTHING as a variation of some precedent. It's been my experience that the lawyers are usually closer to the truth. You really don't need computers to encrypt bookie's records - bookies have been doing that by hand for years. (Perhaps you can figure out the quantities of money, but no bookie worth his salt leaves customer's names in his records in any recognizable form.)

In fact, you don't need to consider encryption AT ALL in deciding whether the Fifth Amendment applies in cases like this. Consider, for example, an arrested man found in possession of an unmarked key to a safety deposit box. It's very, very likely that the box contains valuable evidence. Can he be compelled to reveal where the box is? I don't know, but I'm sure similar cases have arisen over the years.

-- Jerry

Search RISKS using swish-e

THE RISKS DIGEST

Forum on Risks to the Public in Computers and Related Systems

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

Volume 4: Issue 26

Wednesday, 10 December 1986

Contents

Computer Error Endangers Hardware

Nancy I. Garman <ngarman@venera.isi.edu>
Wed, 10 Dec 86 08:44:43 PST

I work for a group that also manages an offsite computer center. There has been so much difficulty with the contractor who is supposed to keep the floor clean that our hardware folks were worried about disk drive contamination from the dirty floor.

I spoke with the Director of Sales for the cleaning company. He blamed their computer for the dirty computer room floor that was risking damage to our disk

drives. Apparently, their computer had us erroneously scheduled for fewer cleanings than our contract called for.

Of course, it is likely to be a data entry error. Still, it makes me wonder - what does their computer have against our computers?!

- Nancy Garman
NGarman@VENERA.ISI.EDU

"One of the Worst Days Ever for Muni Metro, BART"

Peter G. Neumann <Neumann@CSL.SRI.COM>
Wed 10 Dec 86 17:38:57-PST

(From an article by Harry W. Demoro and Carl Nolte in the San Francisco Chronicle, 10 December 1986, p. 2.)

"... doors, signals, switches, brakes, and even a speedometer broke."

The worst mess began at 6 a.m. when an electrical short circuit caused a "ghost train" to appear on the signaling equipment that guides Muni Metro streetcars in and out of the Embarcadero station. [This prevented the switches from working automatically.] Muni troubleshooters did not eliminate the "ghost train" until 8:14 a.m...

By that time BART was a mess... [for the second morning in a row] At 5:10 a.m., a train broke down at the Richmond Yard. Then at 7:10 a.m., the switches that route trains through the MacArthur station in Oakland stuck, creating a bottleneck because two lines converge there. [Workers used hand cranks.] The problem was fixed at 9.07 a.m. Also at 9:07, switches stuck at the Daly City station (18 miles away).

At 7:14 a.m. a door stuck open at MacArthur. At 7:25 a.m. a train was taken out of service because brakes locked for no apparent reason. At 7:33 a.m. a train stalled when the door stuck. At 8:04 a.m. another train broke down in the repair yard. At 8:38 a.m., a train refused to budge because of a stuck door. At 9 a.m the speedometer stuck on a train, which had to be sidetracked. At 10:28 a.m. another train was stalled by a stuck door. The problem "finally cleared itself up at noon," said a spokesman. [Bad Car-ma resolved?]

Things have been fairly smooth for BART and Metro Muni for some time. I don't recall BART having such a disastrous day since 6 years ago. (See Software Engineering Notes 6 1, January 1981) The "ghost train" problem had plagued Muni Metro in its early days, but I had not heard about it recently. (See Software Engineering Notes 8 3, July 1983)

Although the computer systems were not implicated, this "bad day" serves to remind us that when we plan for things not going well, we need to plan for things going REALLY BADLY.

Korean Air Lines Flight 007

Steve Jong/NaC Pubs <jong%derep.DEC@decwrl.DEC.COM>
Tuesday, 9 Dec 1986 11:07:53-PST

In his book "The Target is Destroyed" (1986), Pulitzer Prize-winning writer Seymour M. Hirsh strives to explain why Korean Air Lines Flight 007 flew serenely over the Soviet Union to its doom on September 1, 1983. Since none of the crew survived and the flight recorders were never recovered, any explanation is highly conjectural, but he presents the arguments of a veteran pilot, one who has flown that route many times. After exhaustive studies, including his knowledge of how flight crews work with their equipment, the pilot concluded that a combination of human errors caused the navigational snafu. One of the errors was postulated to be a well-known blind faith in the plane's inertial navigation system (INS).

This triply-redundant, highly accurate system flies the plane automatically once coordinates are entered. The crew enters starting, ending, and "waystation" coordinates into each of the three components. If there is an entry error, or if the plane seems off course, an alarm sounds.

The full scenario is too complex to cover here, but the gist of it is that a crew member fat-fingered the "you are here" coordinates.

How is it a RISK? Consider the anecdotal evidence of other flights:

o Crews place complete faith in INS. They don't have to fly the plane, and sometimes have been known to nap in the cockpit.

o Crews trust INS more than their radar. The pilot who developed this scenario said if the KAL crew looked at their radar and saw the Kamchatka Penninsula where there should have been open ocean, they probably shut off the radar, because the INS was functioning normally.

o The INS is so sensitive that if the plane strays down the wrong taxiway, it sounds off. Crews will shut off the alarm.

o Entry errors are common on long flights, because crews must enter three sets of ten coordinates (over a hundred numbers).

o Though it is strictly against airline policy to do so, at the touch of a button the crew can "autoload" coordinates from one INS to another.

If you accept the scenario, 269 people died at least partly because of blind faith in computers and a tedious interface that was too simply circumvented.

[Reminder: There are quite a few books on this subject. Each tries to justify its own theory, but all seem to come to somewhat different conclusions. PGN]

Plug Compatible Modules; Criminal Encryption

David Fetrow <fetrow@entropy.ms.washington.edu>
Mon, 8 Dec 86 01:45:09 PST

Item 1: Plug Compatible Modules

Concerning the Nurse who accidentally electrocuted a little girl by plugging in AC power to heart monitor electrodes at Seattles' Childrens' Orthopedic.

AP gave the impression that the heart-monitor plug was like a wall-plug. This was not the case: The heart monitor plug consisted of three simple metal probes (like those on an ohm meter). They were accidentally plugged into the slots of the female end of an AC extension cord; which resembled the unit the probes should have been attached to. The solution doesn't change: make unique plugs for everthing around an ICU patient. (Source: KING TV on camera interview with hospital administrator).

Item 2: Criminal Encryption

I remember reading in the Seattle Times a couple years ago about a computer expert who encrypted his kid-porn information on a disk. The police had a warrant for his files but couldn't crack the encryption. They turned to hacker who tried the "decrypt" command without a key. It worked; the evidence was admissible. [No documentation for this one, though.]

More on skyscraper control

Mike Ekberg <weitek!mae@decwrl.DEC.COM>
Fri, 5 Dec 86 17:11:15 pst

One of the buildings in Boston is indeed balanced by computer. I think it is the John Hancock Building.

At any rate, the building was designed by I.M. Pei, a rather famous architect. It was one of the first buildings ever built that is a parallelpiped with non-90 degree angles. The skin of the building is almost solid glass. Soon after the building was finished, glass sheets began falling off the building onto the plaza below. (I don't know if anybody was squashed) This only occured when the wind blew.

An aeronautical engineer at nearby MIT found out why the glass fell. He modelled the building as an vertical aircraft wing fixed on the bottom end. When the wind blows, the wing(building) generates lift on one side. The upper part of the building twists and window dimensions are altered causing the glass to fall.

The solution was to install in the upper floor a large weight controlled by computer. When the computer detects the building being twisted, it counters the torque by moving this weight.

In addition, all the glass in the building was replaced with a type more

resistant to the effects of the building being twisted. The new glass has the property that its optical characteristics are significantly modified when the panes are twisted. In periods of high wind, spotters near the building can monitor its status by using binolculars looking at sections of glass.

mike {turtlevax,cae780,pyramid}!weitek!mae

PS Most of this was related to me by a structural engineer living in Boston.

Satellite interference

James D. Carlson <jc37@andrew.cmu.edu>
Mon, 8 Dec 86 20:06:02 est

From Lauren Weinstein:

> While misaimings and such are fairly common, they rarely result in total
> capture of a satellite transponder, since it takes considerable power to
> completely override the main signal. In the case of the described
> problem with CNN Headline News, the explanation is almost certainly very
> simple and has nothing whatever to do with interfering signals.

Unfortunately, uplink signals are usually fairly weak, about one watt, since they are very narrow beam. The uplink is also frequency modulated, which means that another signal only 1dB stronger aimed in the same direction will take over the satellite's receiver.

(Il)legal Encryption

Richard Outerbridge <outer%csri.toronto.edu@RELAY.CS.NET>
Mon, 8 Dec 86 20:41:18 est

In >The Codebreakers< David Kahn tells of several cases involving crooks, codes and evidence, but none with 5th amendment implications. A related issue is high-order homophonic and "subliminal channel" coding, which are capable of conveying two (or more) legitimate messages depending on the key employed: using Key A out pops Grandma's secret recipe for marzipan; use Key B and out pops the chemistry of the latest designer drug. Even were I legally compelled to divulge my keys, if the analyst can't find 'Key B' how can he prove that I haven't complied by revealing 'Key A'?

Software article in _Computer Design_

<thode@nprdc.arpa>
10 December 1986 0824-PST (Wednesday)

There is an article in a recent issue of _Computer Design_ magazine (the November 15 issue) titled "Approaches to Software Testing Embroiled in

Debate." Its author is William E. Suydam. It covers a lot of the same ground as some of the contributions to this list. Quotations from David Parnas, Nancy Leveson, and others are included. It seems, from my inexpert perspective, to be a decent summary of the problems in software reliability.

--Walt Thode (thode@NPRDC)

Heavy metal and light algorithms

Peter G. Neumann <Neumann@CSL.SRI.COM>
Wed 10 Dec 86 17:31:32-PST

Dave Parnas called my attention to an oversimplification in which I indulged when I noted in RISKS-4.20 that "an algorithm is an algorithm is an algorithm" (This was in connection with Steve Gutfreund's note on encoding algorithms in "smart metals".)

Indeed, Dave is right in suggesting that "the metal algorithm would be, to a very useful approximation, a continuous function or at least piecewise continuous with very few points of discontinuity. As such it could be much more easily analyzed and studied than its counterpart as a digital computer program."

This raises interesting questions about the relative precision, accuracy, and soundness of "metal algorithms" and comparable analog devices in general. The situation is somewhat akin to higher-level programming languages. Perhaps one is less likely to make low-level design and program errors in the directly-implemented analog case, but it is of course still possible to choose the wrong model.

Suit against Lotus dropped

Bill Sommerfeld <wesommer@ATHENA.MIT.EDU>
Wed, 10 Dec 86 13:15:08 EST

The following article may be of interest to Risks readers; it is from page 81 (the first page of the business section) of the Boston Globe of 10 Dec 86.

> Lawsuit charging errors in Lotus software dropped
> By Ronald Rosenberg, Globe Staff
>
> A case seen as a test for settling responsibility when computer software fails was dropped yesterday, a victory for an industry that had stood by nervously as the issue made its way to court.
>
> James A. Cummings, Inc., a Florida construction firm, yesterday ended its suit against Lotus Development Corp. of Cambridge [Massachusetts], a lawsuit that the industry feared could open the door to a host of liability claims against software developers.
>
> In its suit, Cummings had charged that errors in the Lotus software caused

to underbid on, and lost a contract. The company had sought $254,000 in damages from Lotus, a leading maker of personal computer software.

If the case had gone to trial, it would have been the first to question whether a supplier of software tools, such as Lotus, is liable for wrong information produced by users of its programs.

Neither Cummings nor its attorney, John R. Squitero of Miami, will receive anything from Lotus. Squitero, who talked openly about the case last summer, refused to comment yesterday.

Lotus said that under the termination agreement, Squitero and James A. Cummings, president of the Fort Lauderdale contracting company, agreed not to discuss [the] case.

``Lotus is pleased that this attack upon the integrity of Symphony, one [of] our leading products, has ended with the complete vindication of both Symphony and Lotus,'' said Jim P. Manzi, Lotus chairman and president.

Squitero had expected to fly to Boston yesterday to take depositions from Lotus employees. Late Monday evening, Squitero decided to throw in the towel.

``I think they (Cummings and Squitero) hoped that there would be a financial settlement by now, and we persuaded them that we would never settle -- not a penny,'' said Hank Gutman, an attorney with O'Sullivan, Graev and Karabell of New York, which represented Lotus.

Peter Marx, general counsel to the Information Industry Assn., a trade organization for 500 software and computer companies including Lotus, applauded the dismissal:

``Our fear was that as long as the case was hanging out, it might have encouraged creative lawyers to file suits that have no merit.''

Search RISKS using swish-e

THE RISKS DIGEST

Forum on Risks to the Public in Computers and Related Systems

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

Volume 4: Issue 27

Thursday, 11 December 1986

Contents

Computerised Discrimination

Brian Randell <brian%kelpie.newcastle.ac.uk@Cs.Ucl.AC.UK>
Thu, 11 Dec 86 17:45:10 gmt

Perhaps the most worrying feature of the situation described in the following extracts from an article in the Guardian, dated 8 Dec. 1986, is that the computer "was only following orders"!

Claims of Prejudice Against Women and Blacks

MEDICAL SCHOOLS TO FACE DISCRIMINATION ENQUIRY

By Andrew Veitch
Medical Correspondent

Leading medical schools face an investigation into allegations that they are

discriminating against women and black students.
 This follows the discovery by two consultants that their own school, St. George's in south London, has been using a computer selection programme which deliberately down grades applicants if they are female and non-white.
 It is thought that hundreds of well-qualified students may have been turned away on those grounds. The hospital's ruling academic board has scrapped the programme and is likely to launch an internal inquiry when it meets tonight.
 Details of alleged discrimination at St. George's and nine other London schools were sent last week to the Council for Racial Equality, the Equal Opportunities Board, and the Inner London Education Authority.
 "The matter is viewed very seriously," said the CRE's legal director, Mr. John Whitmore. "The commission will be considering the St. George's case on Wednesday and the position of other medical colleges in January."
 An EOC spokesman said there could be a case to answer. Under the Sex Discrimination Act, it is unlawful for a school to discriminate against a woman in the terms on which it offers to admit her, or by refusing or deliberately omitting to accept her application for admission.
 The chairman of Ilea's higher education committee, Mr. Neil Fletcher, considered the allegations at the weekend. Ilea has warned schools that it will withhold grants if they do not comply with its non-discrimination policy.
 The St. George's claim is particularly worrying because the school has a better record on discrimination than most other colleges.
 The computer selection programme was designed to mimic the decisions of the school's panel which screened applicants to see who merited an interview.
 It matched the panel's results so closely that the panel was scrapped and for several years all St. george's applicants have been screened by computer...

Brian Randell - Computing Laboratory, University of Newcastle upon Tyne

 UUCP : <UK>!ukc!cheviot!brian
 JANET : brian@uk.ac.newcastle.cheviot

Belgian Paper transcends computer breakdown

<minow%bolt.DEC@decwrl.DEC.COM>
11-Dec-1986 0844

This appeared on a local [computer-transmitted] newspaper on Thus 11 Dec 1986, as a note from Peter Van Avermaet.

 Today [Wednesday], the Belgian newspaper "De Morgen" has appeared
 as a hand-written newspaper.

 Yesterday morning [Tuesday], the type-setting computer broke down.
 After several hours, it became clear that it would not be available
 in time for today's edition. But "De Morgen" ["The Morning"] apparently
 survives anything - it went bankrupt some weeks ago. Today's edition has
 been hand-written, and printed using the "normal" printing process.

 Some topics:
 graphology,

plans to use more computers in the Ministry of Finance,
for the computation of the taxes we should pay.

Martin

[Goeden "Morgen"! P.]

Re: Plug-compatible modules

"Keith F. Lynch" <KFL%MX.LCS.MIT.EDU@MC.LCS.MIT.EDU>
Wed, 10 Dec 86 23:54:57 EST

Many terminals keyboards have plugs which are the same as modular telephone connectors. I have seen one with a prominent warning that plugging it into a telephone outlet will destroy the keyboard and damage the phone line.

...Keith

Re: Criminal Encryption

"Keith F. Lynch" <KFL%MX.LCS.MIT.EDU@MC.LCS.MIT.EDU>
Wed, 10 Dec 86 23:52:53 EST

I can't see criminal encryption as much of a problem. All REAL crimes involve a victim, who is willing to testify. Perhaps large scale use of encryption will result in government abandoning its wasteful and pointless attempt to prosecute victimless crimes.

...Keith

Re: Criminal Encryption

Thu, 11 Dec 86 09:46:23 -0800

Some crimes involve victims that aren't willing to testify. Blackmail is the classic example; an encrypted blackmail database ensures the victim that his blackmail payments aren't wasted, and ensure the criminal that the incriminating evidence is not easily found (using a needle-in-a-haystack approach).

Dope pushers selling drugs to dope users appears to be a victimless crime also... after all, both parties are (presumably) satisfied with the results of individual transactions. The problem is the activities on the part of both parties to make the transactions possible (theft for the user, bribery and coercion for the pusher) have victims. Law enforcement is always interested in the transactions between pushers (at least) because it usually leads to other agents of victim-ful crime. Thus the interest in data about transactions. Requirements for a secure business relationship between dealers would lead to more attempts to store transaction data securely.

Re: Criminal encryption

Dave Platt <dplatt@teknowledge-vaxc.ARPA>
Thu, 11 Dec 86 12:08:34 PST

Although I'm not a lawyer, I do have an opinion about the question asked recently to the effect of "Could an alleged criminal be compelled to reveal the encryption key for a database containing records related to an alleged criminal enterprise?". My opinion, for what it's worth, is that the courts would probably not uphold any such compulsion, and would likely throw out any evidence obtained by use of a coerced or compelled revelation of an encryption key.

Jerry Leichter suggests (based on a conversation with a lawyer friend) that this situation is analogous to a journalist being compelled to reveal his/her sources. I believe that this analogy is suspect... a journalist is (generally) _not_ under criminal indictment, is _not_ being asked to provide evidence that would incriminate him/herself, and thus the Fifth Amendment does not apply at all. The Fifth Amendment states only that a person cannot be compelled to incriminate him/herself; it says nothing about compulsion to incriminate another person. "Contempt of court" rulings are sometimes used to [attempt to] compel a person to provide testimony or evidence that can incriminate _someone_else_, but they aren't (and can't be) used to coerce a person to provide evidence or testimony that might result in that person's conviction on criminal charges. "Shield laws" are a different matter entirely... they provide journalists with a limited ability to refuse to turn over material in their possession that might possibly reveal the identities of their "sources".

If the prosecution in a particular case chooses to grant legal immunity to a suspect, then the person no longer has the ability to refuse to testify (or provide evidence) concerning matters covered by the immunity, because s/he can no longer "incriminate" him/herself regarding those matters. Prosecutors sometimes grant immunity to a hostile witness (typically a "minor player" in a larger case), so that they can use the threat of "contempt of court" rulings to compel the witness to testify against his/her associates.

Jerry Leichter asks, "Can an arrested man be compelled to reveal where [a locked safe-deposit] box is?". I believe that the answer is "No." The police and prosecution can attempt to locate it themselves; they can obtain a search warrant that will permit them to open and examine the box (or force it open without the key, for that matter); and they can use any evidence found by use of a legal search warrant in court.

By analogy, I believe that in the case involving an encrypted database full of [allegedly] incriminating evidence, the following situation would probably develop: the police and prosecutor could seize the database using a valid search warrant. The same search warrant would permit them to attempt to decrypt the data by brute-force or intelligent-search methods. They could not coerce any of the defendants to reveal the encryption key unless they were first willing to grant legal immunity to that person (either via a voluntary agreement, or via an involuntary grant followed by a contempt-of-court coercion).

Re: More on skyscraper control

Brint Cooper <abc@BRL.ARPA>
Thu, 11 Dec 86 15:01:20 EST

...(a discussion about the skyscraper in Boston which would "twist in the wind" and drop pieces of its glass face to the ground)

> The solution was to install in the upper floor a large weight controlled by
> computer. When the computer detects the building being twisted, it counters
> the torque by moving this weight.

But if the wind is related to a storm which causes a wide-area power outage, perhaps the computer won't be available when it is needed most? Uninterruptible power and backup power are still rather expensive and, I believe, not widely used.

Brint

[It is used where needed -- and can be quite cost-effective, given the alternatives. Hospitals, some banks, and various other applications have realized how important continuous power is. The Network Information Center (SRI-NIC) keeps running despite local power blips that down the rest of SRI's systems! PGN]

The Second Labor of Hercules

Dave Benson <benson%wsu.csnet@RELAY.CS.NET>
Sun, 7 Dec 86 18:43:37 pst

Free copies of the report

> David B. Benson, "The Second Labor of Hercules: An essay on software engineering and the Strategic Defense Initiative -- Preliminary Draft", CS-86-148

are available from the Technical Reports Secretary, Computer Science Department, Washington State University, Pullman WA 99164-1210, by written request, while the supply lasts.

The essay was finished in May, 1986, and has been only slightly dated by events. I intend to begin revising this essay upon the turn of the new year, and would appreciate criticisms from all who would care to send such to me.

Thank you in advance for your cooperation.

Report problems with the web pages to the maintainer

Search RISKS using swish-e

THE RISKS DIGEST

Forum on Risks to the Public in Computers and Related Systems

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

Volume 4: Issue 28

Friday, 12 December 1986

Contents

Mount a scratch giraffe, too? Make that several.

Jim Horning <horning@src.DEC.COM>
Fri, 12 Dec 86 14:17:05 PST

From DATAMATION, Dec. 15, 1986, p. 67

... The Amsterdam air cargo terminal, an enormous, fully automated warehouse, is a major hub where cargo is stored before being routed

to destinations all over the world. In the cargo on any given day are numerous crates of live animals, from dogs and cats to livestock and zoo animals, many of which must be fed during their stopovers. A DBMS is used to keep a mirror image of the warehouse and to track the physical location of all freight traffic.

This system had first been installed by Computer Sciences Corp., El Segundo, Calif., in the 1960s and had worked fine for several years until the DBMS failed. All the data were lost. It took several days and several dead giraffes before the problem was solved, according to Ken Bosomworth, president of Information Resources Development, Norwalk, Conn., who learned of this classic horror story through some former CSC employees.

Elf debuts as parking attendant

Kevin B. Kenny <kenny@B.cs.uiuc.edu>
Fri, 12 Dec 86 15:16:46 CST

From the (Champaign-Urbana, Ill.) Daily Illini, 12 December 1986:

Elf debuts as parking attendant

CONCORD, N.H. (AP)-- Concord's parking elf, captured after a nationwide search, made his debut at the downtown garage Thursday, frustrated by the computerized meter system he was hired to make ``user-friendly'' for the holidays.

``It's flawed,'' said Charlie Bonjorso, a 76-year-old retired barber who answered Concord's call for someone to wear the elf suit.

``You only get 20 seconds' time when you're supposed to remember where you parked your car, have your change ready, and push the numbers,'' Bonjorso said. ``If you're slow . . . that's it, you've lost your money.''

Parking in the garage dropped from 100 percent to almost nothing when a computerized meter requiring a good memory and quick fingers was installed this year, said Ken Lurvey, the city's director of economic development. ``People got confused, they got ticketed and they got frustrated,'' he said. ``It's far from user-friendly.''

Kevin Kenny, Computer Science UUCP: {ihnp4,pur-ee,convex}!uiucdcs!kenny
University of Illinois CSNET: kenny@UIUC.CSNET
Urbana, Illinois, 61801

Plug-compatible plugs

Chris Koenigsberg <ckk#@andrew.cmu.edu>
Fri, 12 Dec 86 10:26:30 est

Someone discovered by accident that the IBM monochrome display adapter will accept a Token Ring connector cable. (Both the Token Ring and the monochrome

display use standard D connectors.) Then, when you power on the machine, the display output brings down the entire local Token Ring that the machine is on. Anyone with a workstation that has a monochrome card can disable their local token ring by plugging the wrong cable into the display adapter (either accidentally or on purpose), and this is good until someone figures out which workstation is causing the outage and removes it from the ring at the wiring closet.

Carnegie Mellon University is wiring all campus buildings, including all dormitories, with the IBM Cabling System. Every room will have at least one outlet. The primary use is to attach personal workstations to the IBM Token Ring. Typically, one or more floors of a building will be running one single token ring. Fun with your dormitory workstation!

Notes:
- Why couldn't they have made the token ring connector a different kind than the monochrome display connector? Did (or should) the hardware design process include any analysis of its consequences in such conjunctions, given known human tendencies?

- With the token ring, it is much easier to isolate the offending workstation and remove it from the network than it would be on an Ethernet. Societal pressures and conventions may evolve to control antisocial network behavior (we hope!).

- Remember when you were an undergraduate, what would you do with a token ring and a workstation in your dorm room?

Plug-compatible plugs

Henry Schaffer <ecsvax!hes%mcnc.csnet@RELAY.CS.NET>
Thu, 11 Dec 86 16:48:02 est

The serial/parallel card on an IBM PC/AT has two (unlabeled) connectors. These are a 9 pin male and a 25 pin (DB 25) female. The owner's manual didn't say which was which - and I wanted to hook up a modem, and I did have a 25 pin male-male cable.

I shouldn't have figured it could be that easy. The nice DB25 is the parallel port and connecting it to a modem damaged it. (The DB9 is the serial port.) I admit I was not as careful as I could have been, but I also feel as if I'd been set up for this.

--henry schaffer n c state univ

An Amusing Article on the Taxonomy of "Bugs"

"Lindsay F. Marshall" <lindsay%cheviot.newcastle.ac.uk@Cs.Ucl.AC.UK>
Fri, 12 Dec 86 08:24:19 GMT

From "The Computer Bulletin" December 1986 by John Lansdown

One of the things Brian [Reffin Smith] touches on in his contribution [to the book "Science*Art"] is the creative potential of software and hardware bugs. He suggests that these might be distinguished from the more bothersome variety by being called, 'pugs'. I have often thought that bugs are as important to us in computing as snow is to Eskimos so, like them, we should distinguish the many different sorts with different names.

To give a few instances. There are some bugs which waylay unsuspecting computer users and beat them into the ground - often fatally: following Brian's example, these should be called 'thugs', particularly as they often arise through the programmer's or manufacturer's misunderstanding of theory. Some bugs are tiresome but the intrepid user can dismiss them as of no consequence: 'shrugs'. All of us have written code that has a special class of bugs which, whilst not being thuggish in themselves, obscure others that sometimes are and hence make debugging particularly difficult: these obscuring bugs should be called, 'fugs'.

Some people claim to write totally bug-free programs - if their programs don't work it is not them that are to blame. The manual, the system or, more likely, the unintelligent user is at fault. Bugs in these programmers' code should be called 'smugs' or, perhaps, 'humbugs'. Bugs which put the system to sleep whilst it still appears to be working or, conversely, make it hyperactive - resulting in reams of unrequired printing or an endless sequence of error messages - should be called 'drugs'. Finally, those which give rise to that undesirable condition known as deadly embrace (brought about by such things as incorrectly designed database lockout mechanisms) should be called 'hugs'.

Only by properly naming these types of errors can we hope to study their true effects and ramifactions. But what should such a study be called? I'd be happy to hear your (printable) suggestions.

[Such a challenge will not go unheeded.
'slugs' might be low-level bugs (like viruses?) that move slowly from one place to another, especially in systems having no shell.
'dougs' might be named in honor of Bell Labs' legendary Doug McIlroy (who with Bob Morris was responsible for EPL, the Multics development-language supersubset of PL/1). Doug used to make multiple patches to the live image of the compiler (which predated the official PL/1 compilers, by the way) ON-THE-FLY, oblivious to compilations in progress. I remember some horrendous (and of course completely nonreproducible) compilations resulting therefrom.
PGN]

Satellite interference

Lauren Weinstein <vortex!lauren@rand-unix.ARPA>
Thu, 11-Dec-86 13:19:16 PST

... "uplinks are only about 1 watt" ...

This is incorrect. Most commercial C-band uplinks (where 99% of the

cable services operate) run in the vicinity of 300-500 watts at 6 Ghz,
usually via a 10 meter diameter antenna. Ku-band uplinks can run
with considerably less power (as low as 20-50 watts under some conditions,
sometimes lower for short-term telemetry-only uplinks) but even these uplinks
will tend to run much more power when they are running a "continuous"
(rather than occasional [e.g. remote news uplink]) service.

Experience has shown that for C-band services (where the studies have been
done to date) it requires on the order of a 10db differential to "capture"
a transponder--lower amounts may cause interference but not capture.
Most uplinks have considerable power in reserve to deal with accidental
(or intentional) interference. In fact, some new techniques have been
developed of late specifically to deal with intentional interference,
some of which are quite clever.

--Lauren--

<"guthery%ascvx5.asc@slb-test.CSNET">
Fri, 12 Dec 86 09:56 EDT

<"ASC::GUTHERY%slb-test.csnet"@RELAY.CS.NET>
To: risks@CSL.SRI.COM
Subject: Fast-food computers

An observation I have made after being subjected to a fair number
of McDonalds and Taco Bell junk-food delivery systems is the following:

> In an evolving man-machine system, the man will get
> dumber faster than the machine gets smarter.

What seems to happen is that people always assume a computer-based system
is smarter than it really is and, as a result, assume they can be dumber
than they really need to be. The result is continuing improvements in the
computer component of the system actually result in a net decline in overall
capability of the system.

When you couple this phenomena with the fact that our schools are turning
out system operators who not only are less well-educated but for the
most part devoid of initiative and common sense (having been pumped up on
gratuitous self-esteem and the notion of a risk-free life), I foresee many,
many more system catastrophes, life threatening and otherwise.

When it comes to improving these systems, I wonder what the impact of
focusing almost exclusively on the computer component of the system is.
Won't the tendency be for the computer component to take on more and
more responsibility? If I, as the designer of the computer part of the
system, am going to be held primarily responsible for its malfunction,
isn't the wise course for me to design for an arbitrarily stupid operator?

The point is that by not regarding system performance as the joint
responsibility of the people and the machines which comprise the system
--- and at least trying to define precisely who is responsible for what ---

those who are to be held responsible will understandably assert the right to build the system as they see fit. You can't put people in the loop without making them liable for the performance of the loop. And yet this seems to be exactly what humanist designers seem to be wishing for.

Re: More on skyscraper control

Chuck Kennedy <kermit@BRL.ARPA>
Fri, 12 Dec 86 4:12:55 EST

Yes, interestingly enough, even such mundane businesses as Sears are now using UPSs [Uninterruptible Power Supplies]. I was recently in the local mall (Whitemarsh) during a heavy thunderstorm and the lights went out. Except in the Sears store where things continued normally. Too bad the rest of the mall didn't have UPSs. (I believe the Penney's at the other end remained lighted as well.)

The connection to computers of this story is, of course, the point of sale terminals that need the juice so that sales can be made. Also, having the lights available makes for less panic. The other merchants in the mall started to close their doors and quickly stationed sales people near them presumably to make sure that nothing "walked off".

I'm not sure what the cost of UPSs is, but if the power shortage were moderately long and happened often enough (we get lots of thunderstorms here at times) I think the UPSs would be worth it. The benefit of being able to continue to conduct business, and not worry about looting, etc. seems well worth it.

-Chuck Kennedy, Ballistic Research Laboratory

Re: Risks of Computer Modeling

<PAX00325%NUACC.BITNET@WISCVM.WISC.EDU>
Fri, 12 Dec 86 01:06 CST

Yes, there are problems in doing empirical work in economics that economists, such as myself, are quick to point out. Verification is done by most, to some degree, but the costs to outside verification are much greater than generally believed. Subtle errors can slip by not only economists, but others as well. For example, in the article to which I am refering to, the name of the professor at UCLA is wrong. E. Leamer is the author of "...Con out of Econometrics."

Craig Paxton, Northwestern University.

Re: Computerized Discrimination

Randall Davis <DAVIS%OZ.AI.MIT.EDU@XX.LCS.MIT.EDU>
Fri 12 Dec 86 19:28-EST

> Perhaps the most worrying feature of the situation described in the
> following extracts from an article in the Guardian, dated 8 Dec. 1986, is
> that the computer "was only following orders"!
> [extract entitled "Claims of Prejudice Against Women and Blacks"]

Perhaps the most wonderful feature of this situation is that it happened and demonstrates one of the powerful beneficial consequences of computers as one vehicle for making knowledge explicit. Discrimination cases are often prosecuted on statistical arguments, which are at best circumstantial and depending on the sample size can be weak. It is very difficult to prove intent and quite rare that anyone admits to it directly. Yet the existence of this program is explicit and direct evidence that the school has in fact been discriminating for however long the program has been in use ("several years") and is interesting circumstantial evidence that the school's panel was in the past doing the same (they agreed that it matched them).

One can only imagine the reaction of the program authors when they discovered what one last small change to the program's scoring function was necessary to make it match the panel's results. It raises interesting questions of whistle-blowing.

The panel is now in an interesting position: they can no longer claim that the admission judgment is "intuitive" or ephemeral: they have themselves agreed that a program captured their behavior. Now that the genie is out of the bottle, it is public and examinable, and that is enormously important. The computer has in this case become an instrument to empower people to enforce equal treatment.

It's quite unlikely that any of this would have come to light in the absence computers and their application to this task; admissions would still be a back-room task carried out with unspoken intuitions and feelings.

Computers and Educational Decrepitude

Geof Cooper <imagen!geof@decwrl.DEC.COM>
Fri, 12 Dec 86 10:17:36 pst

The other day I heard a report on NPR's Morning Edition that the Educational Testing Service had expressed concern about the diminishing literate capabilities of American high school (and thus, eventually, college) students. This concern struck me as ironic, since I consider the ETS the prime backer of a great impediment to literacy, the multiple choice question. Because of the importance (or perceived importance) of the SAT examinations, I believe that modern high school programs have virtually standardized on the use of multiple choice questions to test their students. Tests that in earlier days demanded essays or short, written answers -- tests that challenged not only the student's knowledge of the subject matter, but also his or her literacy -- now demand only smudges on a computer form. Questions that earlier solicited a clear exposition of the student's knowledge of the subject now instead demand that the student distinguish between fine shades of meaning and phraseology. It is my experience that a student who has shown initiative

and learned extra subject material will often find this added information enough to muddle the distinctions between possible answers to the question. The more you know, the worse you do.

The popularity of multiple choice questions stems not from some theory of their importance in education, but from the desire to automatically grade examinations by computer. This brings up a RISK that I haven't yet seen mentioned on the Digest (I haven't been watching it long, so apologies if it has been beaten to death earlier) -- the risk that computers allow for poor solutions to problems by their ability to allow impersonal, centralized institutions to scale up to larger populations.

In the example, above, a desire to produce a standardized test that is given to all students has led to a requirement that the test be multiple choice, so that the exams can be graded by machine. The importance of these tests to the futures of young people has caused high schools to shift their program away from essay questions, so that students' writing skills are not emphasized in every subject, as they once were. The net effect is a societal problem, the decline of literacy in America.

If computers had not been available to correct multiple choice tests, perhaps the ETS would have set up a more distributed testing system, based on certified test graders. Perhaps a wider range of question types would be used, or perhaps oral examinations would have become part of the test. This question is moot, and the answer would not be of pertinence to this digest. The pertinent question does remain:

* Does the ability of computers to process masses of social data encourage poor, centralized, solutions to social programs when distributed (non-computer) solutions would help society more?

- Geof Cooper, IMAGEN

Call for papers - Directions and Implications of Advanced Computing

Jon Jacky <jon@june.cs.washington.edu>
Fri, 12 Dec 86 08:40:51 PST

(CPSR-sponsored symposium in Seattle, July 12 1987)

Call for Papers

DIRECTIONS AND IMPLICATIONS OF ADVANCED COMPUTING

Seattle, Washington July 12, 1987

The adoption of current computing technology, and of technologies that seem likely to emerge in the near future, will have a significant impact on the military, on financial affairs, on privacy and civil liberty, on the medical and educational professions, and on commerce and business.

The aim of the symposium is to consider these influences in a social and political context as well as a technical one. The social implications of current computing technology, particularly in artificial intelligence, are such that attempts to separate science and policy are unrealistic. We therefore solicit papers that directly address the wide range of ethical and moral questions that lie at the junction of science and policy.

Within this broad context, we request papers that address the following particular topics. The scope of the topics includes, but is not limited to, the sub-topics listed.

RESEARCH FUNDING

- Sources of Research Funding
- Effects of Research Funding
- Funding Alternatives

DEFENSE APPLICATIONS

- Machine Autonomy and the Conduct of War
- Practical Limits to the Automation of War
- Can An Automated Defense System Make War Obsolete?

COMPUTING IN A DEMOCRATIC SOCIETY

- Community Access
- Computerized Voting
- Civil Liberties
- Computing and the Future of Work
- Risks of the New Technology

COMPUTERS IN THE PUBLIC INTEREST

- Computing Access for Handicapped People
- Resource Modeling
- Arbitration and Conflict Resolution
- Educational, Medical and Legal Software

Submissions will be read by members of the program committee, with the assistance of outside referees. Tentative program committee includes Andrew Black (U. WA), Alan Borning (U. WA), Jonathan Jacky (U. WA), Nancy Leveson (UCI), Abbe Mowshowitz (CCNY), Herb Simon (CMU) and Terry Winograd (Stanford).

Complete papers, not exceeding 6000 words, should include an abstract, and a heading indicating to which topic it relates. Papers related to AI and/or in-progress work will be favored. Submissions will be judged on clarity, insight, significance, and originality. Papers (3 copies) are due by April 1, 1987. Notices of acceptance or rejection will be mailed by May 1, 1987. Camera ready copy will be due by June 1, 1987.

Proceedings will be distributed at the Symposium, and will be on sale during the 1987 AAAI conference.

For further information contact Jonathan Jacky (206-548-4117) or Doug Schuler (206-783-0145). Sponsored by Computer Professionals for Social Responsibility, P.O. Box 85481, Seattle, WA 98105

Report problems with the web pages to the maintainer

Search RISKS using swish-e

THE RISKS DIGEST

Forum on Risks to the Public in Computers and Related Systems

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

Volume 4: Issue 29

Sunday, 14 December 1986

Contents

<ames!rutgers!seismo!unmvax.unm.edu!wampler@cad.Berkeley.EDU>
Fri, 12 Dec 86 09:07:06 MST

(Bruce Wampler)
To: RISKS@ucbvax@csl.sri.com
Subject: America's Cup: Left-over Digital Filter

This story is from the NOVA "Sail Wars" of 9 Dec 1986:

This NOVA was about the design of Stars & Stripes, one of our entries in the current America's Cup event in Australia. There were two interesting stories, both having to do with modelling and tank testing of scale models.

Apparently in the early 70's, Ted Turner had a boat built directly from a tank model. The boat worked wonderfully in the tank, but was a total dog in full size. This design disaster soured American designers on tank

modelling, ultimately resulting in the loss of the America's Cup 3 years ago to the Australian boat, which had been designed using modelling. In the 70's, the models were apparently on a 1:13 scale.

The current entry was designed using tank modelling (1:3 Scale). Stars & Stripes went through 3 versions. Much of the design was aided by computer modelling, followed by building of scale models for tank testing. The tank testing was closely measured, and the results again fed through computer-analysis programs. The design was getting down to the wire for the 3rd version of the boat. Measurements fed through the analysis programs indicated a serious problem with the stern of the boat. The designers were visibly depressed. After some modifications, new measurements indicated the problem got worse. At this point, they really were out of time - either give up the 3rd version, or find the problem.

In a sort of "sanity test", the designers refused to believe the computer output. This was apparently standard naval architecture software and well trusted, given the reluctance shown to disbelieve the results. At any rate, after a long all-night session, they discovered that "a digital filter used previously for an oil platform test had inadvertly been left in the computer," thus causing the wrong results. With the filter removed, the measurements showed better than expected performance. (Not good enough, apparently. The yacht New Zealand seems to be cleaning up in the challenger races.)

[Moral: Don't forget to change the oil filter. PGN]

Some additions to the "bug" taxonomy

Dick King <king@kestrel.ARPA>
Sat, 13 Dec 86 11:35:12 pst

"mugs" -- Trojan horses and other intentionally introduced anomalies

"plugs" -- interface errors

"ugs" -- a bug isolated to a small piece of code, the sort of thing you can stare at for hours, and all of a sudden someone walks up to ask you if you want to go to lunch, glances at your work, points to the offending line of your CRT or listing, and says "you know, ..."

[ughs?]

Re: uninterruptible power

<TMPLee@DOCKMASTER.ARPA>
Sat, 13 Dec 86 00:41 EST

And in the case of a large installation the back-up power is most impressive. I had a chance to visit Air France's computer center (somewhere near the Riveria) several years ago (pure boondoggle, I admit.) As I recall there were about three floors (basketball court size, maybe) of Univac 11xx's and disk farms (two approximately duplicate systems, each at least two processors) and

comm gear etc. On the ground floor were at least two, maybe three diesel generators that would do a small city proud. Short of a nuclear attack that system was not going to be shut down by anything! (and yes, they made sure the fuel tanks were full and periodically tested the generators -- I don't remember the mechanism used to keep power up while the generators were starting.)

Trade-offs between BMD architecture and software tractability

<LIN@XX.LCS.MIT.EDU>
Sun, 14 Dec 1986 11:48 EST

It has been generally accepted that software for BMD must perform a variety of functions, including tracking targets, discriminating between decoys and RVs, and so on. As importantly, the software must be constructed in such a way that all the parties are confident that it will perform these functions when called upon to do so.

This list of functions raises an interesting point. I agree with the list, but am troubled by its dependence on system architecture. Specifically, we could imagine a "BMD" system that consisted of thick orbiting shells of gravel at 500 km altitude. No ballistic missile now known could penetrate that, and we could have confidence that it would work. The software would not need to perform any of the functions that both critics and supporters of SDI agree must be performed. The sole issue is the cost of putting all that junk in space.

The existence of this "alternative" BMD suggests that the "software" needed to control it need not be complex, extensive or unreliable; the system just proposed doesn't need it at all. However, no one thinks that an actual BMD will not require software. Thus, we conclude that for deviations that are "large enough" from "prototypical" architectures, the software problem can be made tractable. An interesting question arises: How can we develop more precise measures for the phrase "large enough deviations" and the word "prototypical"?

The Eastport Study used such an approach; they said that an unconventional architecture would make the software problem tractable. The argument above suggests that for a sufficiently unconventional architecture, they are right. My problem with the Eastport study is that they have not made an argument that their preferred architecture is even in the right direction of "unconventionality", let alone "far enough"; indeed, I think they have gone in the wrong direction. But my problem with my own position on BMD software (i.e., very critical) is that I have constructed an existence proof that says that in some circumstances, I am wrong.

What are those circumstances? I can't speak in general, but obviously one issue is cost. If you are willing to spend enough money (in the case above, on lift costs), the software problem is tractable. My intellectual question is "Where do I draw the line?"

Re: Criminal encryption

Garry Wiegand <garry@tcgould.tn.cornell.edu>
Fri, 12 Dec 86 23:43:18 EST

I noticed in the paper recently that the former mayor of Syracuse (Lee Alexander??) was fighting a federal court order. The court, on prosecution request, had ordered him to instruct a foreign bank to tell the prosecution all about his bank transactions. The paper said that the ability of the feds to require this was a matter of "settled law"; Mr. Alexander was merely fighting for the privilege of adding the words "under protest" before signing.

Seems like the same rules might apply to other forms of records, such as computer disks. The penalty would be contempt-of-court.

garry wiegand (garry%cadif-oak@cu-arpa.cs.cornell.edu)
Cornell Engineering & Flying Moose Graphics

Computerised Discrimination

"Scott E. Preece" <preece%mycroft@GSWD-VMS.ARPA>
Fri, 12 Dec 86 09:38:09 CST

Brian Randell writes:
> The St. George's claim is particularly worrying because the school has a
> better record on discrimination than most other colleges.
> The computer selection programme was designed to mimic the decisions of
> the school's panel which screened applicants to see who merited an interview.
> It matched the panel's results so closely that the panel was scrapped and
> for several years all St. George's applicants have been screened by computer.

One is tempted to say that the two statements, (1) they were better than average on discrimination and (2) they were following a process that was well modelled by a discriminatory program, are contradictory. Of course, they aren't. Assuming the program was just based on assigning weights to a lot of factors typically used in admissions decisions, it's not hard to imagine that they hit on a set of weights which happened to work well on the training set but were not really reflective of the pre-existing judgment process.

This is dangerous, though, in that it may appear to courts and other bodies that the inference can be drawn; that the existence of a biased model which would explain a behavior is proof that the behavior was biased. This would make the concept of de facto discrimination much more broadly applicable (though it is, in fact, the general basis of that concept).

It does remind one that testing the results of an "expert" system should be coupled with review of its rules.

scott preece, gould/csd - urbana uucp: ihnp4!uiucdcs!ccvaxa!preece

More on Incompatible Plug-Compatible Monitors

<forags%violet.Berkeley.EDU@berkeley.edu>
Sun, 14 Dec 86 15:21:47 PST

It's quite easy to damage an IBM Monochrome monitor by plugging it into an adapter (like an Enhanced Graphics Adapter) which is configured for a color monitor. Both types of monitors use the same D-connector.

Admittedly, there is a warning in the manual about this, but, after setting up about fifteen other PC's, I had pretty much given up reading the manual in detail .....

Al Stangenberger, Forestry, Univ. of Calif., Berkeley

Search RISKS using swish-e

THE RISKS DIGEST

Forum on Risks to the Public in Computers and Related Systems

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

Volume 4: Issue 30

Tuesday, 16 December 1986

Contents

Arpanet outage

Andrew Malis <malis@ccs.bbn.com>
Mon, 15 Dec 86 10:46:48 EST

[An earlier message asked, "Why did the Northeast corridor disappear from the Arpanet last weekend? The Network Operations Center said one trunk had been broken, and they were cut off from most everyone, too. I thought there was enough redundancy in the Arpanet to prevent a single trunk from causing such extensive outage...":]

At 1:11 AM EST on Friday, AT&T suffered a fiber optics cable break between Newark NJ and White Plains NY. They happen to have routed seven [different] ARPANET trunks [all] through that one fiber optics cable. When the cable

was cut, all seven trunks were lost, and the PSNs in the northeast were cut off from the rest of the network. Service was restored by AT&T at 12:12.

The MILNET also suffered some trunk outages, but has more redundancy, so it was not partitioned.

Andy Malis

[Robert W. Baldwin <BALDWIN@XX.LCS.MIT.EDU> noted: This is a classic example of redundancy at one level of abstraction that turns out to be non-redundant at a lower level of abstraction.]

[Redundancy works sometimes: I received several copies of Andy's note. Yes, this is a lovely example. By the way, AT&T is laying a fiber-optic cable under the Atlantic. That will provide LOTS of opportunities for virtually distinct paths to co-occupy the same physical channels. PGN]

Dynamic Signature Verification

Robert Stroud <robert%cheviot.newcastle.ac.uk@Cs.Ucl.AC.UK>
Tue, 16 Dec 86 12:15:20 GMT

There was an article in The Independent recently (2nd Dec 1986) about dynamic signature verification and "the arrival of biometrics as a practical security technology". A company called AI Transaction Security from Cambridge have produced a gadget called Securisign, two of which are being used to control access to "a very secure area" at the EEC's headquarters. [EEC is European parliament]

The article concluded as follows:

"Dynamic signature verification has turned up one disappointment. Researchers originally hoped that signature pads could test the sobriety of people such as nuclear plant operators when they signed on for a shift. However, research shows that most people can sign their names convincingly even when hopelessly drunk". [Copyright (c) 1986 Newspaper Publishing PLC]

I found this last comment interesting because the last time this topic came up on RISKS, I recall that the consensus was that the technology did not work because you had to sign your name very carefully, i.e. not when you were "tired and emotional". However, when I showed the article to Brian Randell, he told me the following anecdote:

Some years ago, I was involved (in an official capacity) in reviewing a research project, at a Laboratory which I would prefer not to identify, on dynamic signature verification. I was given a demonstration of the system, which involved my being asked to sign my name five times, and then being asked to sign again to confirm that the system had now "learnt" and could recognise my signature. Much to the consternation of the demonstrator, my entirely unpremeditated reaction was to turn to a colleague, and ask him to sign my name. Without any prior warning or practice, he roughly imitated what he could recall of my hand movements, without attempting to reproduce the written appearance of my signature. The machine accepted his efforts as

my signature. I was then informed, in tones of considerable embarassment, that in an effort to speed up the demonstration, the thresholds had been set low, and that all would be well if they were reset and I gave an adequate number of signatures. So, they were reset, and I gave (more than) the requested numbers of signatures. To my surprise, the demonstrator expressed surprise when I indicated that I felt it appropriate to repeat my experiment, and again challenged my colleague to repeat his "feat" - something he did immediately and effortlessly!

The point of this story is that this struck me as an elementary check to make on dynamic signature verification systems - yet I do not recall ever seeing claims, in any of the (admittedly popular) articles I have read on the topic, regarding the ability of the system to defeat attacks based on seeing how a person signed his/her name. [End of Brian's story]

Wobbly skyscrapers and passive vs. active controls

Niall Mansfield <MANSFIEL%EMBL.BITNET@WISCVM.WISC.EDU>
Mon 15 Dec 86 17:28:20 N

PGN in RISKS-4.26
> This raises interesting questions about the relative precision, accuracy,
> and soundness of "metal algorithms" and comparable analog devices in general.

If you change the scene a bit and take a mildly absurd example, you could have the same sort of considerations in a desk lamp - either use a normal passive Anglepoise type, or a hi-tech computer-controlled active servo-postioned type lamp. I'd reckon that the old fashioned lamp would behave itself it power cuts (although not very brightly), electrical storms, glitchy mains periods, the last day of february of the year 2000, etc., whereas I wouldn't be at all surprised if the robot lamp went berserk sometime and brained me or smashed my teeth in because the chap next door started radio broadcasting.

For whatever reason - perhaps that we have had such or similar artifacts for centuries - we are confident and "know" that passive devices made of metal tubes and weights and springs are not sensitive to various outside effects which DO affect computers and consequently computer controlled devices, and if only because they behave resonably, (i.e. as we expect them to) such passive devices have a great safety advantage.

Re: The Audi 5000 problems

Matt Smiley <crash!pnet01!msmiley@nosc.ARPA>
Tue, 16 Dec 86 00:52:37 PST

Audi did more damage with the '...there isn't anything wrong.' statement than could be done by simply saying they don't know what it is. Statistically, the rate of such accidents with the Audi should be proportional to the rate of such accidents with other vehicles. It obviously is not, leading me to think there's some defect in the engineering of the vehicle. I had a similar problem

with an old Ford truck of mine, and it took months for me to figure out that it was due to a defective motor mount. The torque of the engine would lift it off the mount and subsequently pull the accelerator linkage to the floor. A similar oddity could be plaguing the Audis.

...nosc!crash!pnet01!msmiley@NOSC <Matt Smiley>

[The summary list of RISKS-4.1 notes that an Audi investigation was reported earlier in Software Engineering Notes, but I just noticed that the reference was wrong: it should have been SEN 11 2 (April 1986). PGN]

Modifying bank cards

Hoffman.es@Xerox.COM <Rodney Hoffman>
16 Dec 86 08:11:51 PST (Tuesday)

From the Los Angeles Times, Dec. 15, 1986 (Reuters):

COMPUTER 'HACKERS' HELD IN W. GERMANY

WIESBADEN, West Germany -- Police have arrested four computer "hackers" said to have robbed banks in the Frankfurt area of more than $50,000 by manipulating cash dispenser cards with a home computer. Hesse State police said the four, one woman and three men, had been roaming Frankfurt and surrounding towns since May with a computer plugged into the battery of their Mercedes limousine. They were arrested at the end of November.

The four hackers bought bank cash cards for $1,500 apiece from their family and friends, who then notified their bank that the cards had been stolen. The four then used their computer to change the codes on the cards' magnetic strip so that they could withdraw more money than the limit set by the cards from automatic tellers, or to tap other accounts. Under a law on computer crime passed last August, the four face jail terms of up to five years if charged and found guilty.

Credit card mag strips

Ted Marshall <blia.UUCP!ted@cgl.ucsf.edu>
Mon, 15 Dec 86 11:45:59 PST

I have noticed a new trend in the way stores imprint credit card slips. In the olden days, the embossed numbers and letters on the card were mechanically transfered to the slip. The only use of the magnetic strip on the back was for verification of the credit limit.

I have now seen two stores (including the local Radio Shack) where the mag strip reader feeds data to an electronic cash register which not only dials-up the bank to verify credit but also prints out the slip for the customer to sign. Unless the clerk checks the printed information on the slip against the embossed card, there is no verification of the information.

Credit card companies are making it harder to counterfit the embossed information on the cards. But a hardware hack can still build a gizmo for $20 that will copy the magnetic information from a "borrowed" card to his. He then makes sure the other card gets returned so that the bank isn't notified. The hack walks into the Radio Shack, buys $1000 worth of stuff with "his" card, and it gets charged to his friend's account. The only thing to trace him with is the signature on the slip, and it's easy to sign your name so that it's close enough for the clerk but no one will ever trace it to you.

Fast-Food Computing

<Edward_Vielmetti@um.cc.umich.edu>
Tue, 16 Dec 86 16:15:04 EST

I must have been in the cycle early for McDonald's fast-food intelligent man-machine systems, according to Guthery's law:

> In an evolving man-machine system, the man will get
> dumber faster than the machine gets smarter.

McDonald's fast food computers (i.e., cash registers) collect all sorts of data on the individual employee at the counter and on all counter sales as a whole. They also do not have a <no sale> key that opens up the cash register, probably to prevent theft. That made it real hard to fix a mistake without calling a manager to get a key to open the drawer.

Solution? Well, the people I worked with at McD's had been around the system long enough to figure out how to get around it. Without getting into too many details of why things were as they were, the easiest way to open the drawer without a manager was to ring up a sale that gave away a tub of barbecue sauce for McNuggets and nothing else.
(Hit <promo> <barbecue> <promo> <total> .)
Of course, that messed up the daily statistics some.

Edward Vielmetti, Ex-McDonalds employee, Computing Center Microgroup, U. Mich.

"bugs"

<doug%btl.csnet@relay.cs.NET>
Sun 14 Dec EST 1986 21:39

plugs Unwanted trash that contaminates output. The classic example is a cheery advertising blurb like "Welcome to MUCUP Version 2.7," which cripples the next program down the pipe.

drugs Unwanted features that contaminate specs; something the cat drug in.

"bugs"

Jonathan Clark <jhc%mtune.UUCP@harvard.HARVARD.EDU>
Mon, 15 Dec 86 11:45:51 EST

At a recent course I heard Jim Gray of Tandem (seriously) describe two more bug types:

Heisenbugs: generally transient failure conditions that exist inside systems. ('I can't let you have this resource now because it has been locked'.) Typically, when the operation is retried on another processor, it succeeds because the backup processor is in a different internal state.

Bohrbugs: repeatable failures even when retried on another processor. Typically these are 'hard errors'.

"bugs"

"ESTELL ROBERT G" <estell@nwc-143b.ARPA>
16 Dec 86 10:05:00 PST

"augs" - induced while augmenting a system.
"dugs" - added while fixing other bugs, digging the hole deeper.
"jugs" - portable bugs, bottled and bonded.
"lugs" - which slow down the system [e.g., security features].
"nugs" - little "nuggets" of gold, which didn't pan out.
"qugs" - errors in queues that make batch jobs miss deadlines,
and print files twice, or not at all.
"rugs" - evenly distributed throughout the code, and pervasive.
"tugs" - little interfaces which keep big systems in tow.
"xugs" - alien bugs [like E-Mail penetrations of UNIX systems]

Search RISKS using swish-e

THE RISKS DIGEST

Forum on Risks to the Public in Computers and Related Systems

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

Volume 4: Issue 31

Wednesday, 17 December 1986

Contents

Don't sit too close! ("And Now, Exploding Computers")

<LEICHTER-JERRY@YALE.ARPA>
17 DEC 1986 16:48:51 EST

From the New York Times (17-Dec-86):

And Now, Exploding Computers

...[T]wo owners of Compaq Portable II computers were rudely surprised recently when their machines simply blew up. The problem, said Jeff Stives, a spokesman for the Houston-based company, arose when service technicians improperly rewired the battery circuits on the computers' main circuit boards.

Compaq engineers managed to blow up another computer in the tests, thus confirming the problem.

In each case the explosion, caused when the machine's lithium battery is accidentally drained of energy and then re-energized by the computer's 5-volt

power supply, was strong enough to break the case of the computer but not potent enough to shatter the glass of the built-in video display screen. No injuries were reported.

Owners of Compaq Portable II computers that have had repair work done on the system board are advised to call Compaq at (800) 847-5785, or call their local dealers for free inspections.

-- Jerry

Car-stress syndrome

Robert D. Houk <Houk@RIVERSIDE.SCRC.Symbolics.COM>
Wed, 17 Dec 86 18:42 EST

From "car" magazine (FF Publishing, 97 Earls Court Road, London W8 6QH), December 1986 issue, "ORACLE" column, page 72

> Electronics are quickly becoming the star of the high-tech society. But they are not without problems. The electromagnetic waves generated by electronic equipment are causing concern among health professionals. Cars are no exception and Professor Kazuo Suenaga of Kurume University has for the first time found scientific proof that electromagnetic waves generated by a car's engine are the cause of car-stress syndrome. According to his findings, such waves from the spark plugs cause nervous stress in the driver and reduces alertness. A device called the Neutral Auto which oscillates micro-electronic waves prevents hazardous electromagnetic waves from entering the passenger compartment, and is said to be effective in preventing motion sickness.

Passed along, with my personal comments pre-censored out. (Actually, the "preventing motion sickness" is conceivable, but the rest sounds rather flaky to me, even allowing for the difference in language 'tween England and the USA.) It would be interesting to see the original paper/report (unfortunately not cited in the column) - maybe someone else out there is familiar with the un-aforementioned paper or Professor Suenaga/Kurume University???

Korean Air Lines Flight 007

Niall Mansfield <MANSFIEL%EMBL.BITNET@WISCVM.WISC.EDU>
Wed 17 Dec 86 10:44:43 N

In RISKS-4.26 Steve Jong, basing his discussion on Seymour Hersh's "The Target is Destroyed" (1986), said:-

> [it was] concluded that a combination of human errors caused the
> navigational snafu. One of the errors was postulated to be a well-known
> blind faith in the plane's inertial navigation system (INS).
>
> ... the gist of it that a crew member fat-fingered the "you are here"
> coordinates.

> ... if the KAL crew looked at their radar and saw the Kamchatka
> Peninsula where there should have been open ocean, they probably
> shut off the radar, because the INS was functioning normally.

Even though Peter Neumann did note that other books have different views on what happened, I think one of the other possible explanations, which exonerates the computers, should still be mentioned.

Very much in contradiction of the quoted arguments above, R.W.Johnson in "Shootdown - the verdict on KAL 007" contends that the plane did not have any INS trouble. Rather, the crew filed flight plans at Anchorage which showed pencilled-in modifications to the computerised flight plan, and that 007's actual course agreed with this modified plan. (Johnson reproduces copies of the plans, which apparently were included in the International Civil Aviation Organisation's report).

Heisenbugs

Rob Austein <SRA@XX.LCS.MIT.EDU>
Wed, 17 Dec 1986 02:03 EST

The recent discussion on Bug Taxonomy reminded me of this one. I may have mangled some of the incidental details, but the gist is gospel.

We have this ITS machine called MC. Its purpose in life is to provide a place to put the big mailing lists for the MIT CS labs so that the other lab machines aren't driven into the ground by the load the mailer puts on the processor. So we tend not to use MC for much else, and COMSAT (the mailer) usually has the machine to itself except when the maintainers are changing something.

Enter a curious hacker who wants to know why MC has not processed any mail for the last 36 hours (this was a holiday weekend, or somebody would have noticed it much sooner!). He pokes around the mail queue directory, checks to see if the filesytem is full, the net is hung, any of the normal things. Finds nothing odd. Finally he examines the COMSAT job with the PEEK program (like TOPS-20 SYSDPY unix ps). Lo and behold, the COMSAT job is now running, the mail queue is being processed, and except for the gap between timestamps in the telemetry file there is no evidence that this ever happened.

After much head scratching amongst the COMSAT and ITS maintainers, we figured out what had (probably) happened. It seems that COMSAT was stuck in a system call, probably doing some network I/O; there was a bug in the code for that system call which caused it to hang forever instead of returning some kind of failure condition. Certain operations involved in examining another job (with PEEK or any other program) cause the examinee to experience a context switch if it is in the middle of a system call: the program counter gets set back to user context, the user context page map and registers are restored, and so forth. This kind of involuntary context switch is a normal event on ITS, and great pains are taken to make it invisible to the user code.

Among other things the program counter and any memory locations that are modified by the system call are updated so that the interrupt is transparent and the job can proceed as if nothing had happened.

So the act of looking at COMSAT broke COMSAT out of the losing system call, and when it restarted the system call it exited properly with an error condition (not surprising, since the machine on the other end of the network connnection presumably had hung up the phone 35 hours and 55 minutes ago).

Did I hear somebody mention the Uncertainty Principle?

--Rob

Heisenbugs

Doug Landauer <landauer@Sun.COM>
Wed, 17 Dec 86 12:19:20 PST

In the rest of the world (most of us don't get to retry our operations on backup processors), Heisenbugs is already a fairly common term -- it refers to bugs which go away as soon as you try to run them under a debugger (or with the debugging compile- or run-time flags set).

Criminal Encryption

Bill Gunshannon <bill@westpt.UUCP>
17 Dec 86 13:44:24 GMT

In his Item 2 (in RISKS 4.26) David Fetrow mentions an incident from a few years ago about a man arrested for kid-porn and the hacker who "broke" his encrypted file for the courts. I think it is time that we finally laid to rest the notion of all these 12 year old hackers out there who are more powerful than a Cray XMP. The article also was printed in TIME magazine and even rated nearly a full page with a photograph of the hacker as well. The fact of the matter is nothing on the disk was encrypted and what the hacker did was public information and being done by micro-computer users all over the country. An explanation follows.

The file the court was interested in was not encrypted, it was password protected and as you might expect the defendant was not likely to freely give them the password. At this point for reasons I can't even imagine they brought the hacker in to the case.

For more background information the computer was a Radio Shack Model III.

Here is an example of a dump of a directory of a disk I created for this demonstration:

```
          file     file name & extension
location  attributes       in ascii
```

```
on disk     \/          \/
 \/  |       |              |
110B00: 0000 0000 0000 0000 0000 0000 0000 0000 ................
110B10: 0000 0000 0000 0000 0000 0000 0000 0000 ................
    |   |   |                  |
      ^   ^          ^
      |   |          |
      |   |     Hash Index Table(HIT)
      |   |
      |   User Password
      |
      Owner Password

110B00: 1000 0000 0046 494C 4532 2020 2044 4154 .....FILE2   DAT
110B10: E042 E042 0000 FFFF FFFF FFFF FFFF FFFF .B.B............

110240: 1000 0000 0046 494C 4531 2020 2044 4154 .....FILE1   DAT
110250: 9642 9642 0000 FFFF FFFF FFFF FFFF FFFF .B.B............
```

There are two passwords for each file, a "owner" password and a "user" password.

The file named "FILE1   DAT" is not password protected.
The file named "FILE2   DAT" is password protected.

A quick look at the directory entry for each file shows you the location of the passwords in the entry. The passwords are not really encrypted. They are merely hashed. This allows an 8 character password to be stored in 2 bytes(1 word on this machine). It also means that any given 8 letter combination will always hash to the same value. The entry for no password is 8 spaces(ASCII 32). All that means is by changing the entry for the "owner" and "user" passwords on "FILE2   DAT" to the same thing as you see for "FILE1   DAT" you have effectively removed the passwords.
This information was provided in numerous magazines like "80 Micro" and "Kilobaud" which had wide readership in the early days of microcomputers. The reason the information was provided was because companies like Tandy and Microsoft distributed their software on single sided disks which was what a store bought Radio Shack computer had in it. But most people(read hackers) who used their machines seriously had modified them to use 80 track and double sided disks. Because of passwords that were not published it was impossible to just copy such as Microsofts Fortran Compiler onto another disk. With the release of this information all one had to do was remove the passwords and copy the files to any media desired.

As you can see there is nothing spectacular about what was done. It was done a regular basis in homes all across the country. But what I see as a problem and why I think this information is applicable to RISKS is that it got so much coverage in the press and served to take a large group of the public who are already uncomfortable or afraid of computers and their effect on day to day life and fed the fires. Here we are 2 years later and this story is still showing up and what is worse is that it will become more fantastic in time as the facts become less and less known. There was no mention of encryption in the TIME article. But as you can see with encryption being on everyones mind today the story has gone from "boy breaks password" to

"hacker breaks encryption".

bill gunshannon

UUCP: philabs!westpt!bill PHONE: (914)446-7747
US SNAIL: Martin Marietta Data Systems RADIO: KB3YV
USMA, Thayer Hall AX.25 KB3YV @WA2RKN-2
West Point, NY 10996

Taking the "con" out of econometrics and computer modeling:

"John Michael (Mike) Williams" <JWilliams@DOCKMASTER.ARPA>
Wed, 17 Dec 86 14:55 EST

a correction and a plea
To: risks@CSL.SRI.COM

In RISKS-4.28, Craig Paxton, identified as an economist from Northwestern University, observes that "E. Leamer" is the correct spelling of the UCLA economist's name, not the "Edward Learner" I used. I double-checked the Science article, and discovered, with the aid of a co-worker, that it is indeed "Leamer," something my increasing far-sightedness could not distinguish in the proportionally-spaced Science typefont: "rn" and "m" continue to look alike through my (obsolete) prescription.

My apologies to Professor Leamer, Science, and the RISKS readership. Despite considerable effort on my part (and the moderator's), an error got through that was caught, finally, by peer review.

Professor Paxton compares this "subtle error" to those in economic verification. No one can consider the 91% error rate measured for modeling of short term oil price changes a subtle error, especially in models sold to or used by the Government to influence major economic policy. A stopped clock is not subtle. Bob Estell, in RISKS-4.25, has it right when he suggests the ACM, IEEE, et al. should require supporting data be archived and retrievable, even if not published with the article in question, so that peer reviewers may at least have some basis for determining reproducability, much less validity or error rate.

In fact we in computers should help pioneer such archives for scientific validation and peer review generally, since initial publication itself is increasingly a computer-based enterprise. RISKS, but for lack of referees, is a prototype of the future journal whose articles must be assessed, reproduced, validated, and archived.

The proprietary arguments do not impress me: if there are those who wish to hide their methods in the name of profit, then they needn't publish in scientific journals, nor expect scientific endorsement. Let them make a fortune, but let them be regarded with the same skepticism that authors of "Get-Rich-Quick" books and newsletters are: if you're so smart [about money, economics, etc.], how come you ain't rich? How come you're peddling books, or models, instead of profiting from the

contents thereof?

I believe there are many ACM, IEEE and other society officials who are regular readers and sometime-contributors to RISKS: may we hear from them?

o First, have they sampled their own publications, as the Journal of Money, Credit and and Banking was, to find what percentage of findings, in computer modeling or otherwise, were reproducible? Do they have policies about surrender of data, equations, etc. on peer request? Do they find the falsification of data and experiments plaguing the biomedical community at the moment to be a problem in computer science publications?

o What actions will they take against authors/papers/presenters who refuse to supply information for reproduction, or validation, or who have falsified, stolen, or otherwise misapplied data and/or findings? What policies do they have on authorship of papers, and are its journals free of the misrepresentations of the number, contribution and even identity of authors, so serious in other fields that even the Wall Street Journal of last week had a front-page story on this problem in AIDS research?

o What is their comment on the challenges for reform in my article in RISKS-4.21, and the additional suggestions by Estell noted above?

Let me ask the readership to forward copies of this discussion to those officers of societies they may know, who are, or should be, able to set or adjust policy on these matters. As a member of ACM since 1964, and in correspondence with an ACM Committee, I would expect at least a comment from ACM as a society.

Search RISKS using swish-e

Report problems with the web pages to the maintainer

Search RISKS using swish-e

THE RISKS DIGEST

Forum on Risks to the Public in Computers and Related Systems

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

Volume 4: Issue 32

Thursday, 17 December 1986

Contents

EXTRA! British Telecom pay phone Phonecard broken?

Peter G. Neumann <Neumann@CSL.SRI.COM>
Thu 18 Dec 86 11:25:17-PST

Britain is currently just at the tip of an iceberg regarding an apparent vulnerability in its debit cards for British Telecom pay phones. The debit cards can be purchased from all sorts of shops, and come in a range of denominations such as 5, 10, 40, or 100 calling units. The system has been in use for a year or two, and card pay phones are both widely accessible and very popular. (If you've ever tried to use coins in a London call box, you know that it is quite an experience.)

My best guess is that it has a holographic stripe, and that a destructive write is used effectively to burn out a part of the hologram corresponding to each message unit -- making it difficult to ADD units to the card.

Unfortunately, a relatively simple doctoring of the card has been discovered that threatens the whole scheme, and makes a card indefinitely reusable [at least until the system is either modified or withdrawn].

An article appeared as the front-page lead story in The Sunday Post (West Scotland?), 14 December 1986, with the banner headline "DIAL WORLD WIDE FOR NOTHING -- TELECOM HIT BY 'PHONE FRAUD'". The article notes that the trick was discovered by a British soldier "fed up with paying a fortune to call his Scottish girlfriend". The word is now spreading around British troops, and can be expected to be widely known in a very short time. (The newspaper states that they know how it is done, and have proved that it works. It cites a variety of calls that they were able to make without any debit to their card.) The consequences of the propagation of this trick are awesome to contemplate.

The system was presumably billed as "foolproof". But "foolproof" is not good enough against intelligence -- although it should be pointed out that the card is not a smart-card in the usual sense. There is no user identification number required, and no use of encryption. The AT&T credit card number seems somewhat safer, as it is quickly revocable on an individual basis. On the other hand, the convenience of the BT phone card is certainly appealing.

A challenge is presented to RISKS as to how to handle this situation. My philosophy is generally to treat the existence of such cases relatively openly, in the hopes that those who need to be protected will become wiser fast enough to act accordingly. If the vulnerability is about to be replicated elsewhere, then knowledge of it may stave off disasters in about-to-emerge applications of the technology. Thus it seems germane at least to call your attention to the problem at this time.

On the other hand, there is a more sensitive question about whether RISKS should divulge specific details of the vulnerability. (Indeed, several possible approaches immediately come to mind, although I do not know the technique that was allegedly demonstrated.) Intelligent discussion on this topic is welcomed here. Furthermore, if hard knowledge of the penetration method is already appearing in the British press, then it would seem to be suitable for inclusion here. I hope some of our British correspondents will keep us informed.

We have previously had some discussions in RISKS on whether to address operating system and network flaws, where it is vital that vulnerabilities be quickly known to system personnel -- the flaws may already be widely known elsewhere. It might be tempting to think that the holocard situation is small peanuts -- it is only dealing with 10P at a crack. But that can add up in a hurry when people discover they have unlimited free dialing. It might alternatively be tempting to think that this situation is more sensitive than computer system security flaws, e.g., because MONEY is involved -- namely defrauding British Telecom. But many computer systems control very large sums of money, and are vulnerable to much greater frauds than pay phone ripoffs. At any rate, stay tuned, and let's see what happens.

It is certainly of concern to RISKS to point out that most such schemes have vulnerabilities that transcend the set of assumptions made by the designers. This appears to be a case in point.

There are also risks in smart-cards (widely used in France), although the frauds are not quite so easy to perpetrate.

[Thanks to Donn Parker for having brought back with him a copy of the Sunday Post whose presence all over a newspaper kiosk caught his eye as he was leaving for his flight back from London on Sunday. It is pure coincidence, I guess, that he travels the world hunting down and consulting on computer related crime!]

Search RISKS using swish-e

THE RISKS DIGEST

Forum on Risks to the Public in Computers and Related Systems

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

Volume 4: Issue 33

Sunday, 21 December 1986

Contents

Help British Telecom save a WORM.

Scot E. Wilcoxon <sewilco@mecc.UUCP>
21 Dec 86 04:01:49 GMT

> >Unfortunately, a relatively simple doctoring of the card has been discovered
> >that threatens the whole scheme, and makes a card indefinitely reusable [at
> >least until the system is either modified or withdrawn].

A read-after-write test before using the resource (telephone time in this case) might be the generic solution. This won't work if the BT reader can't be positioned to read what has just been written. Hopefully there aren't many other major installations with the same flaw (BART & other transport?).

Computer programmers should know of this flaw due to one eagerly-awaited peripheral which is finally becoming available. Writeable optical data disks (ie, WORM drives) promise storage of huge amounts of data. People who want to sell large numbers of programs or data will now be able to put hundreds of

programs on one optical disk. One "demonstration disk" method being used by some companies is to allow a program to be used a few times or for a few days. This method may be vulnerable to a write-blocking technique similar to the British Telecom card doctoring, although different physical tools may be needed. The designer of an optical disk collection should be aware of this technique so he can thwart it.

Scot E. Wilcoxon Minn Ed Comp Corp {quest,dayton,meccts}!mecc!sewilco
(612)481-3507 sewilco@MECC.COM ihnp4!meccts!mecc!sewilco

security of magnetic-stripe cards [This relates to earlier risks.]

Brian Reid <reid@decwrl.DEC.COM>
20 Dec 1986 0109-PST (Saturday)

There are three ways that I know of to fraudulently modify magnetic-strip credit cards. The technology to make mag-stripe credit cards secure against two of them has existed for almost 15 years. Most credit-card companies do not use it because it is more expensive than the losses that they are currently sustaining from fraud. However, the main reasons for its expense are that it requires new card-reader electronics, and in the fullness of time one could imagine moving to it.

The three attacks are:
1) Copying the strip from one card to another
2) Modifying the contents of a card with read/modify/write (or rewriting it completely, if you choose)
3) Making a checkpoint of a card, using it, and then restoring the card to its former state.

This technology can protect against attacks (1) and (2), but not (3). I first heard about it from a security person at the National Bank of Washington in 1973.

Here's how it works. When a credit card is molded, it is molded out of plastic that has had nickel particles stirred in with it. The magnetic strip is affixed, and the card is run through a machine that senses the location of the nickel particles on the card and computes a cryptographic checksum of their positions. The checksum function is secret. That checksum is used as the decryption key of a 2-way encryption function, and the remaining information on the magnetic strip is encrypted in such a way that the nickel-particle checksum of the plastic card is used as the decrypting key for the data on the magnetic strip.

This protects against attack 1, copying, because the contents of the mag strip on one card will not work on a card with a different nickel checksum. This protects against attack 2, forging, because even if the forger can determine the position of the nickel particles he does not know how to compute the checksum from their position. It is easy to design a system for which attack 3 will not be useful.

I believe that the expense of this system is the expense of the particle-sensing readers, which are more delicate than mag-strip readers. I am confident that if electronic fraud with credit cards starts to cost more than the particle readers, that banks will switch.

Brian Reid
DEC Western Research

Korean Air Lines Flight 007 (RISKS-4.31)

Dick King <king@kestrel.ARPA>
Thu, 18 Dec 86 13:48:36 pst

I'm very unimpressed with the straightness of the logic in Shootdown. There seem to be as many contradictions within that volume as there are in the record of the shootdown itself.

As one example, on page 24 [hardcover, American edition] he states that "The full significance of this becomes apparent if one realises that Soviet ground control was undoubtedly monitoring 007's conversation with Tokyo, presumably with a slight lag as a translation was obtained. ...". The transcripted conversation, to which the Soviets were "undoubtedly" listening, clearly identified the airliner as 007. The thrust of P. 24-27 is that the plane gave out deceptive information that fooled the Soviet air defence. On page 187, however, he quotes the Times as quoting US intelligence analysts as saying "the initial identification of the the jetliner as a military reconnaissance aircraft became fixed in the mind of Soviet air defence officials and was strengthened after Soviet interceptors were unable to locate the plane for two hours".

Mr. Johnson did not explain why the Soviets were, according to him, listening closely enough to this routine airliner traffic to be fooled, and why, if they thought the intruder was not 007, they attributed 007's broadcasts to this intruder. Remember, they were supposed to be hearing 007; they are just supposed to have thought that this plane wasn't it.

-dick

Car-stress syndrome (RISKS-4.31)

Dick King <king@kestrel.ARPA>
Thu, 18 Dec 86 12:19:22 pst

This brings up an interesting RISK imposed by high technology in general -- namely that certain people will take advantage of the public's natural fear of the unknown. They can either offer new and different forms of snake oil or, as this ad seems to do, or they can prey on the public ignorance as to how things work and what is known or not known about safety and levels of exposure, to attract a following for whatever reason.

What has this to do with computers? Two groups I know of are arguably using

this tactic in a computer-related manner. One group, 9-5 I believe, attempts to bolster a political base by causing CRT's to be regarded as *unsafe*. The second group offers to clear credit problems, doing nothing you couldn't do for yourself [per CR], but implying in at least some of their ads that they have an "in" with the computer network.

-dick

* I will apologize to the first person who can show me that most of the group's supporters refuse to allow a TV into their homes, or at least that the group advocates such refusal. I have never even seen any such literature claim that monochrome TV's are safer. This would be obviously counter-productive because most of the intended audience uses monochrome monitors, but voltages are lower, images are crisper, flyback noise tends to be less; this covers most of the claimed problems with CRT's.

Bugs called cockroaches [A True Fable For Our Times]

<anonymous@erehwon>

[THE FOLLOWING WAS CONTRIBUTED FOR ANONYMOUS INCLUSION ON THE GROUNDS OF SEVERE AUTHOR EMBARRASSMENT AT EVER ADMITTING TO WRITING SUCH AWFUL DRIVEL (EVEN THOUGH THE INCIDENT DESCRIBED IS ABSOLUTELY TRUE) OR TO INCLUDING SOME HORRIBLE PUNS (MOST OF WHICH HAVE BEEN REMOVED BY THE SOMETIMES IMMODERATE MODERATOR).]

> Heisenbugs is already a fairly common term -- it refers to bugs
> which go away as soon as you try to run them under a debugger
> (or with the debugging compile- or run-time flags set).

I once had an amusing problem where the most likely cause was that I was exceeding array bounds. Naturally I turned on the bounds checking flag, and got fatal output errors. So I next put in manual traces, and I still got fatal output errors. Highly annoying, no? A little investigation revealed that the newly compiled-in format strings were getting trashed. I'm talking about a genuine cockroach.

What to do, what to do? I declared a dummy array of dimension 100k--what the heck, it was on a Cray--so from then on the array overflow was safely trashing the dummy; I got my trace and I killed the nasty little bugger.

So, what is the moral of this story? Obviously,

"Rough strings do flake the darling bugs of Cray."

[Ah, yes, the iambic pentameter is always a giveaway. For those of you in search of the original, the first line is exceedingly well known:

Shall I compare thee to a summer's day?
Thou art more lovely and more temperate:
Rough winds do shake the darling buds of May,
And summer's lease hath all too short a date:

...

I hope that any future shaggy bug stories will be more lovely,
more temperate, and less anonymous. PGN (LE KOOK or HOTSHOT?)]

Re: More on car computers (not Audi)

Controls Wizard <dma%euler.Berkeley.EDU@BERKELEY.EDU>
Thu, 18 Dec 86 12:09:35 PST

According to the latest issue of Consumer Reports there is a recall of 1982 Toyotas because a problem with the cruise-control computers can result in uncontrollable acceleration. Yet another reason for Audi to rethink their position.

Miriam Nadel [Specify by name in any direct reply]

Runaway Audi 5000

"John O. Rutemiller" <Rutemiller@DOCKMASTER.ARPA>
Sat, 20 Dec 86 11:03 EST

The Washington Post Magazine for December 21, 1986 had an article in which the author supports Audi's position of driver error. I believe his view helps show the current trend of people like "60 Minutes" to blame a computer or machine without looking at operator error. I'm glad someone is willing to accept possible operator error. The full text follows.

Audi's Runaway Trouble With the 5000, by Brock Yates

I recently watched in fascination as Ed Bradley reported on the CBS-TV show "60 Minutes" that the 1978-'86 Audi 5000 sedans can treacherously launch themselves like misfired missiles when their automatic transmission levers are placed in drive or reverse. This phenomenon labeled "unintended acceleration," has allegedly been responsible for several deaths, including a particularly poignant one - tearily documented on the show - in which a pretty young mother crushed her young son against the back wall of a garage. The segment included testimony from several victims. They decried Audi's suggestion that the trouble lay not in a mechanical flaw but in driver error.

Audi says the drivers accidentally hit the accelerator, not the brakes, after engaging the transmission. Although Bradley acknowledged Audi's explanation and interviewed two of its engineers, he clearly sided with the owners.

"60 Minutes" portrayed the Audi 5000 as a flawed automobile, perhaps cursed by its "idle stabilizer control," a fuel system component that supposedly triggers "transient malfunctions" without warning.

But wait a minute, did Bradly tell us everything? There is no arguing the Audi is in serious trouble with the 5000: Sales are down 20 percent

and the Center for Auto Safety has taken the position that the Department of Transportation should require Audi to buy back all its 5000s. Further, an Audi spokesman agrees that "hundreds" of acceleration incidents have occured in the 5000s. The Center for Auto Saftey has received 500 reports and believes more than 750 reports have been made altogether. Audi has ceased to stonewall the issue. "We take the responsibility to resolve the problem," says Audi public relations director Ed Triolo.

Furthermore, the phenomenon of "unintended acceleration" is not new. The problem has occurred in a variety of autos with automatic transmissions. More than 2,000 complaints have been made about General Motors models built between 1973 and 1986. Owners of Toyotas, Renaults, Mercedes-Benzes and Nissans have also reported unintended acceleration incidents. However, the Audi 5000 has the highest percentage of acceleration incidents: about 1 in 400 cars built.

Triolo says that in the 270 accidents that have been examined by Audi engineers, only six idle-speed stabilizers were found defective and not in a way that would cause rapid, unexpected acceleration. More important, the Audi 5000 - with its 2.2-liter, five cylinder engine developing only 110 hp - simply does not have enough power to override its brakes. (Drivers involved in the incidents swear they are standing on the brakes. Audi has found no instances of brake failure in autos it has examined.)

Who's right? Will an Audi 5000 outmuscle its own brakes? I borrowed a 1984 Audi 5000, floored the accelerator with my right foot and stepped on the brake hard with my left foot. Then I moved the transmission from park to drive. AND THE ENGINE STALLED! It lacked sufficient power to override the brakes. According to my brief test, for unintended acceleration to occur, two independent systems - fuel supply and brakes - must fail simultaneously and somehow return to normal.

Audi says it went even further. In demonstrations for both CBS and NBC, it made full-throttle acceleration runs to speeds between 30 and 50 mph and then, with the throttle on the floor, stopped the car with the brakes.

All of which raises some interesting questions "60 Minutes" failed to ask about the Audi 5000 incidents:

Why, after millions of starts over an eight-year period, haven't there been any runaway 5000s reported at Audi's 410 dealerships?

Why do there seem to be more of these incidents among drivers who have relatively little experience driving the Audi 5000? (There are an inordinate number of such incidents within the first 2,000 miles of the life of a given car.)

Why are there no reported accidents with the Audi 4000 Quattro, which has an identical idle stabilizer mechanism?

Why do independent experts, who have speculated that the trouble is centered on throttle linkage, the computer brain in the engine, the

automatic transmission or the idle stabilizer, still openly admit there is no obvious culprit?

Why, in a number of accident investigations, did Audi engineers find the accelerator pedal bent, even snapped off, presumably by foot pressure?

While continuing to research the incidents, Audi has so far installed 32,000 interlock devices that prevent the transmission from being engaged without the driver's foot on the brake. Audi has asked all owners of the 5000 model to bring their cars in for free installation of the interlock. Audi is adamant that the device is a solution, although Triolo says the company does not expect it to eliminate the problem.

Drivers of three cars equipped with the interlocks have reported runaway crashes. In the first case, an Audi spokesman says, the driver's description of the event changed over time, and Audi representatives decided it was not a case of brake failure or runaway acceleration. In the second case, Audi says a bushing was installed upside down, preventing the interlock from working. In the third case, Audi says it has not been allowed by the owner's attorneys to inspect the vehicle.

Audi contends that the problem of unintended acceleration is a complex one involving a number of factors, including the design of the car itself, the driver, and external distractions. Triolo says the problem of unintended acceleration is inherent in automatic transmission cars throughout the auto industry, not just in Audis.

There is one potential explanation for the runaway Audis that strikes me as obvious: The brake and accelerator pedals in the Audi 5000 are off-center, to the left. In models of the 5000 built before 1983, it was even possible to step on the brake pedal and the accelerator at the same time, a problem Audi has since rectified. Audi maintains that brake and accelerator pedals in autos come in a wide range of placements, some farther to the left than Audi's.

I maintain the pedals are sufficiently misplaced that inexperienced drivers might easily thrust a right foot forward and hit the accelerator when intending to hit the brake. Audi has investigated at least one incident in which a 5000 was driven a foot or so into a concrete wall in a parking garage, the rear tires spinning in anguish, the driver confused as to what was happening until she finally realized her right foot was on the accelerator.

Sadly, one of the most troubling aspects of these incidents is that so many Audi 5000 drivers fail to avert disaster simply by shoving the transmission shifter into neutral or turning off the ignition. While it certainly is understandable that a panicked driver might actually press harder on the throttle of a runaway car, thinking he was stepping on the brake pedal, such a reaction also exposes the dismal training and minimal presence of mind the average American driver has when faced with an emergency.

How about a segment on driver training, Mr. Bradley?

Search RISKS using swish-e

THE RISKS DIGEST

Forum on Risks to the Public in Computers and Related Systems

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

Volume 4: Issue 34

Tuesday, 23 December 1986

Contents

Debit cards that don't (RISKS-4.32)

Edward M. Embick <embick%tetra@nosc.ARPA>
Mon, 22 Dec 86 14:05:59 PST

I, like others, can only guess at the mechanism used to "debit" the card in question. However, it would seem to me that a mechanism so designed would also reread the card to ascertain the debiting action was taken. If not, disconnect! I suspect that the design of the system was made simple and cheap, and the design reviewers committed one of the fundamental analysis flaws that introduces risks to a system. They reviewed the basic design, and assumed that since the device is designed to work that way, that unless it breaks, which will be apparent, it will only fail by misreading

the card, which will only happen in an acceptably small number of cases where the call costs more than is on the card.

This mindset is the same that most peer groups and outside analysts get after analysing a system for possible fraud or abuse. They tend to profile a community of potential system users and a range of views of the system, and overlook the obvious vulnerability of a new, but in their minds, trusted part of the system, because the card has passed the test and is out of the user's physical control.

Ed Embick (the more paths I make, the more paths they break! waaaaaaa....)
Computer Sciences Corp. embick@noscvax.UUCP or
4045 Hancock St. {decvax,ihnp4,ucbvax}!sdcsvax!noscvax!embick
San Diego, CA 92110 (619) 225-8401 x516 MILNET: EMBICK@NOSC

British Telecom Phone Cards (RISKS-4.32)

Peter G. Neumann <Neumann@CSL.SRI.COM>
Tue 23 Dec 86 11:28:58-PST

I had a call from British Telecom about their Phone Card, but I was not around to receive it. Despite the newspaper story to the contrary, they apparently insist that their Phone Card was not compromised, and that the British Post reporter must have misunderstood what he was told when he described the free-call scam and when he perpetrated his allegedly free calls. Stay tuned, and maybe we'll have more later.

Edward Embick points out an intrinsic security vulnerability that results if such a system assumes that WRITES always succeed, so that they don't bother to READ after an attempted (DESTRUCTIVE) WRITE to see if the write worked. This leaves them open to monster vulnerabilities that sooner or later might be exploited. The speculative list of possible attacks is most interesting, and keeps growing.

Re: security of magnetic-stripe cards

<hplabs!pyramid!utzoo!henry@ucbvax.Berkeley.EDU>
Mon, 22 Dec 86 18:44:47 pst

> ... The technology to make mag-stripe credit cards secure against
> two of them has existed for almost 15 years...
> ... The checksum function is secret...

Around this point the alarm bells start ringing. How long will it *stay* secret? Not forever! The safest approach would probably be to burn it into custom hardware at central sites (*not* in each reader, because it's impossible to maintain physical security on thousands of readers) so that programmers don't have routine access to it. Even then it will probably get out eventually, unless you shoot the people who lay out the chips after they finish.

The technique *would* be a major short-term obstacle to magstripe fraud.
But it would not make magstripe cards permanently secure against fraud;
it would stop fraud only for a while, and merely make it harder thereafter.

Henry Spencer @ U of Toronto Zoology
{allegra,ihnp4,decvax,pyramid}!utzoo!henry

Plug-compatible plugs

<hplabs!pyramid!utzoo!henry@ucbvax.Berkeley.EDU>
Mon, 22 Dec 86 18:45:20 pst

> Someone discovered by accident that the IBM monochrome display adapter will
> accept a Token Ring connector cable...
> - Why couldn't they have made the token ring connector a different kind than
> the monochrome display connector? Did (or should) the hardware design process
> include any analysis of its consequences in such conjunctions, given known
> human tendencies?

It does in other areas. In avionics design, it is normally mandatory that
no two functionally-different plugs be physically identical. This is
usually achieved by keying systems rather than by a vast inventory of
slightly-different connectors, although there are quite a variety used.

The crucial difference is that avionics systems are, to some degree, designed
around the assumption of imperfect maintenance. The military in particular
has to contend with complex systems maintained by ill-trained technicians
subject to many distractions (e.g. gas masks, bombs falling nearby, etc.).
Unfortunately, the healthy paranoia that this induces in designers doesn't
seem to be present in the computer business.

Computer systems have been designed around the assumption of perfect
maintenance for quite a while, actually. The cables used to connect most
disks and tapes to their controllers are physically but not logically
symmetrical, with no keying. At least a 180-degree rotation from one end
to the other isn't generally destructive, the stuff just doesn't work!
Still worse are symmetrical female connectors which plug onto rows of pins
protruding from boards: not only is it possible to get the connector on
the wrong way, but it is also possible to get it misaligned with the pins,
so that some pins stick past, rather than into, the connector. The grid of
pins is regular and symmetrical -- they are normally on the 0.1-inch square
grid that is standard for all manner of electronic components -- and there
often is no housing around them to constrain the plug to fit in only one
place. Slightly fattening the plug to prevent pins sticking past it would
solve this, but nobody seems to bother. Even some prefabricated sockets
which *do* have outer plastic shells are roomy enough that a narrow plug
can go in misaligned by one row of pins. (I speak from experience.) The
D connectors used since time immemorial for RS232 lines, and increasingly
common for all manner of things on personal computers, at least lack these
flaws.

There is no great mystery about why this stupidity occurs: it's cheap, and

nobody can be bothered improving it. The offending connectors are available from a wide variety of competitive sources, and are available in "mass-terminated" forms that can simply be clamped onto flat cable without the expensive and largely manual operation of soldering individual wires into the connector. A grid of pins sticking up from the board is cheaper than a prefabricated connector. It's cheaper to put the pins on the standard grid than on a special one that would interfere with improper connections, and cheaper to buy female connectors that have all holes present rather than having one blocked off for keying. And so forth. Often it's possible to get at least some degree of protection if one tries -- keyed mass-terminated connectors do exist, for example -- but all too often suppliers don't bother. Even something as simple as making one socket male and the other female offers at least slight protection against wrong hookups.

Henry Spencer @ U of Toronto Zoology
{allegra,ihnp4,decvax,pyramid}!utzoo!henry

Runaway Audi 5000

Mark Brader <mnetor!msb@sq.arpa>
Tue, 23 Dec 86 14:19:42 EST

The Washington Post article posted by John O. Rutemiller is indeed an interesting response to the original 60 Minutes story, but it does not cover two points mentioned -- though not stressed -- in that original story.

1. One of the drivers who was interviewed after the runaway-accident said that he had *both* feet on the brake. From the pedal sizes as seen on 60 Minutes, it isn't possible to fit both feet on the accelerator.

2. The common description of the accident was that the transmission was shifted out of Park and then the engine ran away. Now, when I shift a car out of Park, I normally step on the brake first or not at all. How come the drivers of runaways are shifting out of Park and *then* stepping on the pedal?

Mark Brader utzoo!sq!msb [* New Address! *]

Ozone layer

Mark Brader <mnetor!msb@sq.arpa>
Tue, 23 Dec 86 18:11:28 EST

The delayed discovery of the recent reduction in the atmospheric ozone layer was discussed earlier in RISKS. Readers interested in a 1-page summary of what is now known, and the competing theories, can find this in the January 1987 Scientific American at pages 67-68. Mark Brader

---

Another heisenbug

Zhahai Stewart <gaia!zhahai%ncar.csnet@RELAY.CS.NET>
23 Dec 86 08:25:06 GMT

If we haven't driven the heisenbugs (bugs that change or disappear under examination) into the ground yet, I will contribute yet another. I once had a simple program which ran (or didn't run) under CP/M on an early microcomputer. Under the debugger, it ran fine, of course. I traced the problem to the following. I had reversed a conditional jump instruction, causing the program to take an early quick exit. Under normal conditions CP/M put the regular return-to-system address on the stack before calling a program, so one could just return for a shortcut exit. Under the debugger, the stack was relocated to just below the program, with nothing in it. Thus the program popped the first two bytes of code as the return address. This turned out to be exactly the address after the misdirected conditional jump - continuing the execution normally and terminating with a more robust method. I was more than usually bemused by this coincidence; it also served as the inspiration for some tricky schemes to thwart disassemblers.

Zhahai Stewart {hao | nbires}!gaia!zhahai

More "bugs"

Richard Lamson <rsl@CERRIDWYN.SSF.Symbolics.COM>
Tue, 23 Dec 86 12:23 PST

Date: Tue, 23 Dec 86 10:06 EST
From: Tom Parmenter <parmenter@STONY-BROOK.SCRC.Symbolics.COM>

Here are some alternate attempts. If we just take the -ug words that already exist in American, we get

dug - documentation bug
fug - bug that causes you to give up (fug it)
hug - deadly embrace bug
jug - bug that can get you jailed, such as penetrating security or spelling Ada lowercase
lug - big, lovable bug (e.g., Unix)
mug - bug that drives you to drink
pug - bug that makes you want to go in the boxing ring with its author
plug - bug that keeps a system going
rug - bug that knocks the system flat
slug - bug that slows everything down, leaves a trail of slime, and eats up your lettuce
smug - bug you can't find
snug - bug that you put in for job security
tug - bug that you can't forget, no matter how many years ago it was

[OK, OK. I think I have to pull the rug out from
further contributions, unless they are outstanding.
This one gets through because it's Christmas. PGN]

Computer Malpractice

Dave Platt <dplatt@teknowledge-vaxc.ARPA>
Mon, 22 Dec 86 18:05:41 PST

The 1/87 issue of High Technology magazine has a one-page article (p.61) entitled "Safeguarding against computer malpractice". It doesn't go into great detail but is probably worth reading.

One point the article's author makes is that the concept of "software malpractice" has evolved fairly recently, and is tied to the transition of SE from a "skilled tradesman" discipline to a "professional" one.

Financial Servomechanisms

Brian Randell <brian%kelpie.newcastle.ac.uk@Cs.Ucl.AC.UK>
Tue, 23 Dec 86 15:43:35 gmt

[We have had various fragments on this before. This one seems to add a little more, but I have not tried to axe out the duplication... PGN]

SOFTWARE STRIKES IT RICH
(From The Observer, London, 21 December 1986)

Computers have produced at least two major crashes on the New York Stock exchange this year, and are set to repeat the process on exchanges around the world, causing wild oscillations in exchange rates.

Computer programs in the US are set up to look for discrepancies between the price of a futures contract on a stock index and the price of the stock that makes up the index. When the price falls, the stock price tends to fall more slowly than the futures contract.

The programs spot the discrepancy, sell the stocks and buy the futures to make a risk free 'arbitrage' profit. The process is called program trading. It caused a shudder in the Dow Jones Index in March, when a number of futures contracts 'unwound' at once, and again in September, when the index fell 86 points one day and 34 the next.

Software company Data Logic has come up with a program which will spot these discrepancies on any index with a futures contract anywhere in the world. The program will also spot discrepancies between the futures contract on the currency the stocks are traded in and the spot and forward rates of that currency.

For example, a program on a computer in Chicago - which is the world capital of futures and program trading - could spot discrepancies between UK stock prices and the contract on the Financial Times/Stock Exchange 100 Index.

It would sell stock and buy the futures contract, amplifying any fall in the index. This would precipitate a run on sterling, the program would then spot the discrepancy, sell sterling, buy the futures contract and drag the sterling rate further down.

The fortunes freed by US banks to play these markets are phenomenal. Wells Fargo Investment Advisors, which ISN'T one of the major players, has $3 billion ([pounds]2 billion) available for arbitrage trading. Morgan Stanley in

New York are rumoured to have made more than $1 million on one program during the first half of this year.

'On an average day, around 25-33 per cent of the trading on the big board (at the New York Stock Exchange) is done through programs,' says John Blin, former chief executive of the NYSE. 'But when there is a severe mispricing the volume can exceed 50 per cent, or around 75 million shares.'

Regulators at the US Securities and Exchange Commission are trying to cut down the level of program trading by bringing forward the time futures contracts mature to an hour before the exchange closes.

The next step for Data Logic is to tie in a market predictor program to the arbirage spotting program. Data Logic's market predictor, ISFX, has been operating in one London bank for most of the year. It uses a database built up from various sources - economists, regression analysis, charts - and weighs these against actuality to predict future movements in the sterling/ dollar spot market.

The company has a deal with the bank so it gets a percentage of the profits made from using the program. In the three months since this arrangement was concluded, Data Logic's development costs have been more than covered.

The plan is to 'sell' to eight or nine banks in The City, but to tailor it to the individual bank's ethos.

But, however much Data Logic tries to deny it, eight or nine ISFX programs built by the same programmers might well simultaneously come to the same conclusion quite often, so precipitating major movements in the exchange rates. If all these programs act simultaneously, and enough cash is freed by the banks for them, then ISFX's prophesies will be self fulfilling, making effective control of exchange rates impossible.

The program is now being extended to cover the Deutschmark/dollar markets then to sterling/Deutschmark forward rates and so on. A similar system predicting movements on the gilts and money markets is being developed by software house Dealing Systems.

JASON NISSE

Brian Randell - Computing Laboratory, University of Newcastle upon Tyne
UUCP : <UK>!ukc!cheviot!brian
JANET : brian@uk.ac.newcastle.cheviot

Search RISKS using swish-e

THE RISKS DIGEST

Forum on Risks to the Public in Computers and Related Systems

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

Volume 4: Issue 35

Saturday, 3 January 1987

Contents

Computer Gets Stage Fright

Chuck Youman <m14817@mitre.ARPA>
Fri, 02 Jan 87 10:14:36 -0500

The Washington Post reported on December 29 and 30th that the Sunday matinee and evening performances of Les Miserables at the Kennedy Center Opera House were cancelled due to a malfunction of a massive rotating stage that is used in the production. An estimated 4,600 theatergoers had paid between $22.50 and $40 for their tickets would get a refund or have their tickets exchanged for another show. (The show is sold out through the remainder of its run, however). Some patrons were reported to be angry because they thought they would be unable to get a refund for their parking ($4) in the lot in the center. It was reported the next day however, that the parking fees would also be refunded. It was estimated that each cancelled show could result in losses of up to $60,000.

The failure was reported to be in a computer that controls the turntable. The turntable covers most of a 40-foot-wide stage, revolves both clockwise and counter-clockwise, and at various speeds. When the components in the circuitry are not working properly, it can take off at full speed. It is used at one point to hold two huge scenery pieces each weighing more than three tons, not counting the cast members standing on it. Because they are computer controlled and so hefty, technicians were unable to arrange a safe method of manually moving them around the stage. (I'm not sure I would call the automated method safe, however.) The reported problem was a faulty electronic circuit card that interfaces the computer with the turntable drive mechanism. The nearest replacement card was in Chicago. It arrived Monday and Monday's performance went on as scheduled.

Charles Youman (youman@mitre)

[It is apparently not true that To the Victor, Hugo, Go the spoils! PGN]

Still More on PhoneCards

Peter G. Neumann <Neumann@CSL.SRI.COM>
Wed 24 Dec 86 09:36:03-PST

I had a call from Colin Sex at British Telecom at 5PM Christmas Eve GMT. He stated that "The card itself is completely secure." They indeed do a READ-AFTER-WRITE check (along with some other checking), so that part of it looks OK. However, there are problems with physical damage to the laser reader/writer. In the case at hand, nail polish had been caked onto the card, and gummed up the works. But in such cases the unit is supposed either to reject the card, or else keep the card if it cannot eject it -- and then shut down. I think they are still vulnerable to some active-card attacks, but on the whole they think they protect themselves well against the man on the street.

Miscarriages Up in Women Exposed In Computer-Chip Process

Martin Minow, MSD A/D, THUNDR::MINOW <minow%bolt.DEC@decwrl.DEC.COM>
27-Dec-1986 2323

(For the record, this item does not represent the opinions of my employer. Martin Minow)

Associated Press Wed 24-DEC-1986

Digital Miscarriages Study:
Miscarriages Up In Women Exposed In Computer Chip Process

HUDSON, Mass. (AP) - Significantly more miscarriages have been found among women production workers at a semiconductor plant than those not exposed to processes used in making computer chips, a study has found.

In one principal area of production, the level of miscarriages was twice

that of non-production workers, according to the University of Massachusetts' School of Public Health study commissioned by Digital Equipment Corp.

The findings, believed to be the first of its kind in the computer industry, has broad implications for the computer chip industry, which employs more than 55,000 U.S. production workers, with most believed to be women.

The study, which found no evidence of a wide range of other major health disorders such as birth defects and infertility, surveyed 744 of Digital's nearly 2,000 workers at the Hudson semiconductor plant. Of those studied, 294 were production-line workers and the rest were non-production workers.

The study, based on the history of the workers at the plant for five years, was designed to measure a wide range of possible health problems among women and men. In all, 471 women were studied and 273 men.

Among the non-production workers, the study found that 18 percent of the pregnancies resulted in miscarriages, similar to the general population.

The incidence of miscarriages among production workers involved in what is known as photolithography, however, was 29 percent. A variety of solvents are used in the process, which involves printing circuits on computer chips.

Among workers in a phase of production that uses acids in an etching process, researchers found a miscarriage rate of 39 percent, twice that of the control group.

Digital said it immediately passed along the findings to its workers.

``We've kept our employees informed all along,'' spokesman Jeffrey Gibson said Tuesday. He said Digital adopted a policy during the study of encouraging pregnant production workers to seek transfers.

As a further precaution, Gibson said Digital also is offering to transfer any female production worker of child-bearing age to non-production work if they have concerns about future pregnancy.

Gibson said Digital decided to do a study after employees began noticing increased cases of miscarriages among their colleagues.

Digital and the researchers stressed that the link between production-line work and increased miscarriages was only a statistical one and that no causal relationship between the health and specific chemicals had been established.

The Semiconductor Industry Association, headquartered south of San Francisco, said Digital sent it a summary of the findings and that the information was passed along to 60 of its computer chip manufacturer members.

``The reaction (of manufacturers) was that the firms all felt an obligation to communicate the information about the study to their employees,'' said Shelia Sandow, association spokeswoman.

The full study, conducted by Harris Pastides, an associate professor of public health at the University of Massachusetts in Amherst, and Edward Calabrese, a professor of toxicology, is still going through review before publication in a medical journal.

But Digital officials said they received a copy of the study last month, and felt, along with its authors, a responsibility to release at least a summary of the findings because of the health concerns.

Across the Atlantic with Cast Iron

<Boebert@HI-MULTICS.ARPA>
Wed, 31 Dec 86 09:53 CST

I am appealing to RISKS readers because this is clearly the polymath's forum

... I am collecting instances of generic pathologies in engineering project management, such as cutting the budget for tools (example: Brunel's ship the Great Eastern, stranded on the banks of the Thames for months because the money men would finance the ship but not the launching equipment. This was the Victorian equivalent of funding the software but cutting out the debugger.) In this vein, I recall seeing a classic case of Victorian Vaporware, to wit, a proposed cast iron bridge over (I believe) the North Atlantic. This was in a book titled "Great Dreams of Victorian Engineers," or some such. Anybody else recall this? When I get the instances together I will submit them to this list as an aid to separating risks which are computer-specific from those which have been around since the dawn of engineering.

Heisenbugs -- Two more examples

"Maj. Doug Hardie" <Hardie@DOCKMASTER.ARPA>
Wed, 24 Dec 86 11:12 EST

I am reminded by the chain of discussions on Heisenbugs of two interesting occurrences that I have been involved with. The first occurred while in college with an IBM 1620 (the last one IBM maintained). One day while the system was running student jobs, the operator was helping me prepare for a microbiology test (flunkout class), the disk drive stopped functioning. The entire system locked up and we investigated. There was nothing detectably wrong, the system just wouldn't make the disk work. Since it was under full IBM maintenance, we called them. However, the only person they who had ever worked on that type of machine was a senior manager and was out of the area on vacation, they sent the next best. This tech arrived some time later and began to try and figure out how it was supposed to work and what was going on. Since I was an EE, I "helped" him. I learned a lot, he learned that there was nothing wrong - it just didn't work. After several hours, he finally gave up and came and sat on a bench by me where I had returned to microbiology. All of a sudden, the disk heads jumped, the process picked up as if nothing had happened, and the system was back in operation. We tried everything imaginable to make it fail again. It continued to work fine for several hours. At that point, the tech packed up his tools, tore up his time card, and left with the statement that he had never been there.

The second occurred a few years later on a military program that used a militarized processor. I had a contractor developing software and as usual they were quite late. So they took the step of scheduling work around the clock. One Monday morning a programmer came in complaining that he had lost his weekend time. He was scheduled from 1200 - 1300 on Sat. Just as he got on at 1200, the machine started slowing down. The lights on the front panel blinked slower and slower until they stopped. Nothing he did made it start running again, until 1300 when it started back up as if nothing ever happened. Needless to say, his management was not convinced. However, when someone else came in the next Monday with the same story, they decided to investigate. The next week they reported it to me with the same lack of appreciation. However, since the machine was GFE, we were responsible for its proper operation. So I got some higher-ups to contact the vendor to fix it. The vendor stated that such was absolutely not possible. It took

several weeks to force them to send a tech out. Sure enough when they did, it performed exactly as advertised. After 1300 when it came back up, the tech started to leave without saying anything. We cornered him by the front door. All he would say was, we've seen this before - it will go away. He was right, it went away after a few more weeks.

Risks Involved in Campus Network-building

"Wombat" <rsk@j.cc.purdue.edu>
Wed, 24 Dec 86 09:44:10 EST

This little scenario popped into my mind after reading Chris Koenigsberg's comments on plug-compatible plugs in RISKS 4-28.

Imagine a university campus utilizing local area networking in academic buildings, dormitories, and other locations. Now picture someone with a reasonable aptitude for understanding the principles of LANs, and with motivation to subvert the campus LAN...and whose dorm room contains a wall socket marked "Southwest Campus Ethernet".

What can this person do, assuming that other people are using this same physical network, and perhaps that this group of people extends beyond those whose nodes are actually on the network to those whose nodes are sending or receiving packets that are being routed over this network (without their knowledge, assuming that they don't monitor packet routing)?

It seems quite plausible to me that such a person could tap into the Ethernet and grab interesting packets (the person down the hall's report on its way to a central printer; private correspondence between two residents; perhaps a test in preparation being sent from a TA to a prof), and send interesting packets (same as above, with slight modifications).

[Lots of passwords are flowing as well... PGN]

Further, it doesn't seem too unlikely that this scenario could be extended; what could two or more people do in cooperation? What goodies could be pulled off the wire if one used a semi-smart program (say, a keyword searcher) to examine traffic for interesting items? Could an entire campus network be crippled by a few malicious users with access to the hardware? (I think the answer to this is "yes".)

The human consequences could be widespread and difficult to cope with; what recourse does the student whose term paper disappeared off the network have? How does one show that a student cheated on a test by gaining a copy the night before via the network? What obligation does the university have to ensure the privacy of electronic mail over a network it designs, builds, maintains, and supports for student use? [Side question: could the campus police monitor electronic mail for suspicious actions without a warrant? After all, the senders of mail put their letters on a public (withing the university) network...]

My opinion is that the kind of widespread network-building that's going on at some colleges and universities is premature; it's a nice idea to build an

electronic village on campus, but peaceful villages have a habit of getting overrun by barbarian hordes from time to time. I'm waiting for the day when the news comes that someone at CMU or Brown or wherever has done something very antisocial with the campus network. (Note that I distinguish between those academic networks where access to the hardware is not provided, or is at least made difficult to obtain, and those which purposefully provide hardware access in many places.)

Rich Kulawiec, rsk@j.cc.purdue.edu, j.cc.purdue.edu!rsk
Purdue University Computing Center

Update on Swedish Vulnerability Board Report (RISKS 3.85)

Chuck Youman <m14817@mitre.ARPA>
Fri, 02 Jan 87 15:56:10 -0500

In RISKS-3:85 I referred to an article that appeared in Signal magazine on "Computers, Vulnerability, and Security in Sweden." I have since written to the author of that article, Thomas Osvald, and he sent me an English summary of a report by the Swedish Vulnerability Board titled "The Vulnerability of the Computerized Society: Considerations and Proposals." The report was published in December 1979. The complete report is only available in Swedish. If anyone is interested in obtaining the complete report I now have a mailing address to obtain publications made by the Vulnerability Board (which no longer exists).

The vulnerability factors considered by the Board included:
-Criminal acts
-Misuse for political purposes
-Acts of war
-Registers [i.e., databases] containing information of a confidential nature
-Functionally sensitive systems
-Concentration [geographic and functional]
-Integration and interdependence
-Processing possibilities in conjunction with the accumulation of large quantities of data
-Deficient education
-Defective quality of hardware and software
-Documentation
-Emergency planning

The original article in Signal magazine mentioned a project by the Board that addressed the vulnerability problems associated with the complexity of EDP systems. This particular study is not mentioned in the summary. However, Mr. Osvald also sent me a copy of a position paper he authored on the subject titled "Systems Design and Data Security Strategy." Some excerpts from the paper follow:

> Whether we like it or not our society is rapidly becoming more complicated, not the least as a consequence of the extremely rapid development of information processing and data communication. Our times are also characterized by increasingly large scale and long range decisions and effects. Unfortunately, this development does not correspond to a similar

progress in our human ability to make wise decisions. It is therefore important that we recognize the limits of the human mind and our ability to to understand and process complicated, long range, decision problems. If complexity is not understood and kept within reasonable limits we will not be able to control developments and we will become slaves rather than masters of our information systems.

What are the characteristics of excessively super-complex systems? One important symptom is that even experts find it hard or impossible to understand or comprehend the totality of such a system. The inability to comprehend is not an absolute criterion that does or does not exist but rather a vague feeling - mainly of uncertainly. This basically goes back to the well-known fact that the human mind cannot deal with or keep track of more than about seven objects, entities or concepts at a time. Above that number, errors in the understanding and problem solving process increase disproportionately.

Why are such systems designed? I can think of three possible reasons. The first is a strategy error of systems development that may be called "revolutionary change" or "giant step approach." During the seventies some large, administrative government systems were re-designed in order to take advantage of new data processing and communication technology. At the same time, as part of a huge "total" project, organization and administration were redesigned - all in one giant revolutionary change. A better and more successful approach would have been - as it always is - to follow a step-by-step master plan where each step is based on previous experience and available resources.

The second reason is the sometimes uncontrolled, almost cancer-like growth of large administrative systems, without a master plan and without clear lines of authority and responsibility, in efforts to integrate and to exploit common data.

The third reason is the inability of systems designers to identify the problems of system complexity and our own inability to handle complex systems and to set a limit to growth and integration.

Charles Youman (youman@mitre.arpa)

DES cracked?

Dave Platt <dplatt@teknowledge-vaxc.ARPA>
Fri, 2 Jan 87 17:51:56 pst

There's an interesting article in the 1/87 issue of Radio-Electronics which states that the Videocypher II television-scrambling system has been cracked. As Videocypher depends in some part on the DES cyphering algorithm, this may have some major implications for computer-system security (if it's true).

According to the article, "perhaps as many as several dozen persons or groups have, independent of one another, cracked Videocypher II and we

have seen systems in operation. Their problem now concerns what they should do with their knowledge."

As I recall (and I may well be wrong), M/A-Com's Videocypher II system uses two different scrambling methods: the video signal is passed through a sync-inverter (or some similar analog-waveform-distorter), while the audio is digitized and passed through a DES encryption. Information needed to decrypt the digital-audio is passed to the subscriber's decoder box in the one of the "reserved" video lines. The actual decryption key is not transmitted; instead, an encyphered key (which itself uses the box's "subscriber number" as a key) is transmitted, decrypted by the decoder box, and used to decrypt the audio signal.

I've heard that it's not too difficult (in theory and in practice) to clean up the video signal, but that un-DES'ing the audio is supposed to be one of those "unfeasibly-difficult" problems.

I can think of three ways in which the Videocypher II system might be "cracked". Two of these ways don't actually involve "breaking" DES, and thus aren't all that interesting; the third way does.

Way #1: someone has found a way of assigning a different "subscriber number" to an otherwise-legitimate M/A-Com decoder, and has identified one or more subscriber numbers that are valid for many (most?) broadcasts. They might even have found a "reserved" number, or series of numbers, that are always authorized to receive all broadcasts.

This is a rather minimal "crack"; the satellite companies could defeat it by performing a recall of all subscriber boxes, and/or by terminating any reserved subscriber numbers that have "view all" access.

Way #2: someone has found a way of altering a decoder's subscriber number, and has implemented a high-speed "search for valid numbers" circuit. This could be done (in theory) by stepping through the complete set of subscriber numbers, and looking for one that would begin successfully decoding audio within a few seconds. It should be pretty easy to distinguish decoded audio from undecoded...

This way would be harder for the satellite companies to defeat; they'd have to spread the set of assigned subscriber numbers out over a larger range, so that the search for a usable number would take an unacceptable amount of time.

Way #3: someone's actually found a way of identifying the key of a DES transmission, with (or possibly without) the unscrambled "plaintext" audio as a starting point.

This I find very difficult to believe... it would be difficult enough for one person or group to do, let alone "perhaps as many as several dozen... independent" groups. Naturally, this possibility has the most severe implications for computer-, organizational- and national security.

I suspect that the reported "cracking" of Videocypher II is a case (or more) of Method #2, and thus doesn't have immediate implications for

the computer industry (I think).

Has anyone out there heard of any other evidence that DES itself has been cracked?

Disclaimer: I don't own a TRVO (or even get cable TV), and have no financial interest in anything related to the TVRO or cable industries.

Second disclaimer: as the Radio-Electronics article points out, it's horrendously illegal to own or use any piece of equipment that "tampers with DES or attempts to profit from decoding it" (the article suggests that such action would be legally equivalent to treason, as DES is/may be under the protection of the NSA until 4/22/87). I don't know where such devices might be purchased.

Search RISKS using swish-e

Report problems with the web pages to the maintainer

Search RISKS using swish-e

THE RISKS DIGEST

Forum on Risks to the Public in Computers and Related Systems

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

Volume 4: Issue 36

Tuesday, 6 January 1987

Contents

A Heisenbug Example from the SIFT Computer

Jack Goldberg <JGOLDBERG@CSL.SRI.COM>
Tue 6 Jan 87 11:25:55-PST

The following hardware bug was found in the debugging of the SIFT fault-tolerant computer. The memory was built of static RAM chips, in which the memory cells were flip-flops. Due to a defect in manufacture, the cross-coupling of the flip-flops in some of the cells was capacitive rather than conductive. The effect was that the cells behaved perfectly when exercised ("observed") frequently, but when information was stored and not revisited, the charges on the cross-coupling capacitors would leak off and

the flip-flop would become unstable, perhaps switching state. The quality of the accidental capacitors was high, so it would take about twenty minutes of inactivity (non-observation) for the event to occur. The debugging problem was compounded by the fact that numerous chips suffered from the same manufacturing defect. I won't enumerate all the hypotheses that were tried before the phenomenon was identified.

A similar phenomenon has been found in logic circuits, associated with charge that may accumulate at unused gate inputs that were not properly connected to a holding potential. I am aware of some painful debugging experience that that form caused in another fault-tolerant computer development.

The Heisenberg Risk is evident and easily generalized beyond the chip level (one can imagine analogs at the program level). It has substantial implications for risks to system dependability, because it subverts several conventional models of testing. First, a person who is testing a defective system usually assumes that the defect is due to a fault in the system, that the fault is static, that there is some test (or test sequence) that will reveal it, and that when the test is applied, the fault will be revealed more or less immediately as an observable error. This phenomenon says that there may be some latency in the manifestation of a fault, and that the latency may occur not only after a test sequence has been applied, but after any element of the sequence has been applied.

A second subversion is to the standard practice of testing during manufacture. Chip manufacturers simply cannot afford to let chips stand in their expensive testers for the time it would take to reveal such phenomena, and system manufacturers also have practical time limits for their test exercises. In practice, such faults, hopefully rare, must be found and coped with at other points in the system lifecycle.

More Heisen-debugs

<LINDSAY@TL-20B.ARPA>
Sun 4 Jan 87 22:09:32-EST

I recently encountered a particularly infuriating Heisenbug. A large program, when given a large input, was just mysteriously dying. Of course, I ran it under the debugger. The mystery deepened: the program returned quietly to the debugger. I say "mystery" because the call stack had been unwound, and yet my breakpoints at the various exits were not reached.

My first reaction was to place a trail of breakpoints, with the idea of seeing how far it got. Some results were obtained, but each time I tried to refine the result, with a new set of breakpoints, the problem seemed to have moved elsewhere.

The clue came when I tried to read some of the debugger's online documentation. The (VMS 4.1) debugger refused to talk, and instead gave me a message about a lack of resources. Aha ! The next step was to have an operator increase my resource allocation (actually, my maximum number of IO operations). I logged out, I logged in, and the problem was gone.

I have harsh words to say about an operating system which will kill a job, without leaving any evidence that it did so. But, I leave these words to your imagination.

I have also had the privilege of a debugging session, done through the communications software which was being debugged. In this case, I have advice to novices. << Keep notes. Good ones. <> Trust me.

Naturally, the hardware world has its share of these things. At one point, PDP-8 maintainers knew that the fix for a certain kind of crash, was to wave your hands near the backplane. (I am NOT kidding. Ask very old DEC hands.)

And then there was the hobbyist 8080 board whose clock worked, but only when a scope probe was applied to the clock line. Turned out that the capacitance of the scope probe overcame the cigar ash under the CPU socket ...

Don Lindsay

The Conrail train wreck

Peter G. Neumann <Neumann@CSL.SRI.COM>
Tue 6 Jan 87 19:16:38-PST

It is too early to write the definitive piece on this, but there are various conflicting reports. The advance warning signal (back two miles on the main track) may or may not have indicated GO (an up-bar) instead of CAUTION (a slant-bar); the crossing locomotive engineer ran his stop signal; the cab crew of the Conrail train had bypassed the emergency alarm that is supposed to go off if they run a signal (as suggested by a PBS interview this evening, which indicated that three separate safety systems would have had to fail simultaneously). Stay tuned for the interpretation of the "event recorder".

Software glitches in high-tech defense systems

Peter G. Neumann <Neumann@CSL.SRI.COM>
Tue 6 Jan 87 19:30:06-PST

An article by Steve Johnson in the San Jose Mercury News (4 Jan 87) listed a new bunch of problems.

* A multimillion-dollar satellite network called "MILSTAR", which is supposed to link the president and top generals with tactical field units in wartime, is months behind schedule because of software troubles... (Lockheed)
* A computerized system intended to help direct artillery fire for soldiers at Fort Ord in Monterey County and other army bases is beset with software delays.
* Two computer projects intended to make it easier to keep track of equipment inventories at the Naval Supply Center in Oakland [CA] and similar installations elsewhere have been held up because of software

development problems.
* Researchers at SRI International in Menlo Park a few years ago were hired to analyze a new "over-the-horizon backscatter" radar system that was supposed to detect attacking planes. They found numerous software errors that meant months of delays in the system.

Elsewhere, the Air Force and Navy have had to postpone changes for the F-16C and F-18 fighter jets because of software hitches... Similar problems have hurt... "LANTIRN" ... and "AMRAAM". [The article also talks about SDI, software costs escalating, and the shortage of (competent) engineers.]

"If we can't get substantial increase in (software) productivity, there is just absolutely no way we can produce the amount of software the defense industry needs in the next few years." (Dorothy McKinney, manager of the software engineering department at Ford Aerospace (FACC) in Palo Alto.

[Thanks to Michael Melliar-Smith for bringing this one in.]

Computer program zeroes out fifth grader; Computerized gift-wrap

Peter G. Neumann <Neumann@CSL.SRI.COM>
Tue 6 Jan 87 19:46:17-PST

Edward Reid dug into his archives for this one, from the Gadsden County Times (FL), 25 Oct 1984. One extra blank space between a fifth grader's first name and his last name resulted in his getting a ZERO score on the sixth-grade placement test. Despite protests from his parents, he was forced to reenter fifth grade. It was six weeks into the new school year before the test was finally regraded manually and the error detected. (The boy cried and wouldn't eat for days after he got the original score of ZERO.)

Edward also produced a clipping from the Philadelphia Inquirer, 5 Dec 1986. Computer printouts of the San Diego Unified School District's payroll somehow did not make it to the shredder, instead winding up as Christmas gift-wrapping paper in a local store (Bumper Snickers). [Perhaps some of the bumper crop wound up in the NY Mets' victory parade?]

Videocypher, DES

<LEICHTER-JERRY@YALE.ARPA>
5 JAN 1987 12:32:58 EST

Dave Platt mentions a Radio Electronics article concerning the breaking of the Videocypher system, and speculates about the implications.

This whole issue got hashed around in sci.crypt a couple of weeks ago. The Radio Electronics article contains a LOT of nonsense, in its claims about the illegality of breaking DES in particular. Also, the claims that DES itself has been broken are not credible.

The Videocypher system has at least two vulnerabilities: Each box contains a chip with a fixed key in it (the same in every box) which, if known, would allow anyone to determine actual working keys and intercept transmissions. Also, independent of the cryptography, the box itself makes a decision as to whether to allow you to see a particular channel.

This allows at least to avenues of subversion: Open a box and read the key from the embedded chip, or take a box and change its decision procedure so that it allows you to see channels you are not supposed to be able to see. (As I understand it, given a valid subscriber key, any box CAN extract the key for ANY channel - it just refuses to work on channels it is not supposed to see.)

With enough equipment, it is possible to open up a chip, dissolve off the epoxy it's embedded in, and read the contents of any PROM with a scanning electron microscope. I gather there ARE techniques for protecting chips against this sort of probing, but they may be too expensive for boxes that are supposed to sell for a couple of hundred dollars. (They may also involve booby traps that would be considered too dangerous in consumer equipment.)

Meanwhile, "rsk" speculates about the vulnerabilities of campus local area networks. This is a REAL concern. Ethernet, and all other LAN's I'm aware of, are completely open to anyone who can gain physical access to them. Listening in to any conversation is easy; spoofing is only a little harder. Yes, problems will arise.

The solution is the use of well-understood cryptographic techniques. As far as I know, while these techniques are understood, there have as yet been few implementations, mainly because of the expense involved. (For many years, billions of dollars a day were transfered "by wire" over telephone lines with no real protection, cryptographic or otherwise. It's only in the last couple of years that concern about security, and technology, have reached the point that these lines have been protected.)

I expect we will see a re-hash of the OS/360 hacker phenomenon. (OS/360 had so many security holes that many people broke into it. It was never really fixed, just replaced.)

-- Jerry

More on the possible DES crack

David Platt <dplatt@teknowledge-vaxc.arpa>
Tue, 6 Jan 87 09:46:20 PST

I just got a copy of the 2/87 issue of Radio-Electronics, which contains brief descriptions of several of the systems that have "cracked" the VideoCypher II scrambling system.

The systems described are all "software" approaches that fall into what I described as "way #1"... they work by cloning copies of an authorized subscriber number. At least one has found a way to crack the "tiered

distribution" feature of VideoCypher, thus permitting someone who has paid for only one service to successfully view several others.

None of the systems described so far actually involve a "cracking" of DES itself... they're all methods of copying an existing (valid) key from one decoder to another. It appears that the MA-Com folks did take some steps to conceal the subscriber number information (which generates the actual key dynamically, I believe), but that their steps were not sufficient. Apparently, the subscriber-number is stored in the battery-backed RAM in a small TI microprocessor, and there's no direct way to query it; during operation, though, it's apparently possible to trace the signals on some of the micro's pins and "catch" the subscriber number as it flys by. Someone has found a way to do this and to "download" the number into the micro in another decoder... thus permitting the "cloning" of an authorized number.

So, the vulnerability of the VideoCypher II system appears to boil down to the fact that its "innards" aren't sufficiently guarded against probing and/or modification. If, for example, the box had been provided with a cover-removal switch that would signal the micro to erase its subscriber number, it might have been more difficult to "crack".

A description of several "hardware" approaches is promised for next month. I'll summarize once I get my hands on an issue.

Campus LANs

James D. Carlson <jc37#@andrew.cmu.edu>
Sun, 4 Jan 87 17:30:26 est

I am a student at Carnegie-Mellon University (Senior, EE) and I therefore speak only for myself, not the Academic Computing Center.

First of all, in our system there are (basically) two types of files: local and network. Local files, like the password file, are only rarely transmitted over the network, and network files are maintained on the file servers. The password file, when transmitted, is in an encoded form anyway. You will never see a raw password floating around the packets, at least they tell me so. Because of the way the network operates, it would be a lot easier to get into the file servers themselves (false authentication, and so forth) than to pick the information up on the net.

To the second part, the University's obligations, I think that they are the same as with large computers. If you used the computer to create a paper, then lost it before the due date, tough! You knew the risks when you requested the account. As to the "wrongful" obtaining of information, such as test questions, anyone who keeps highly sensitive information on a computer in unencoded form gets what he deserves. This is not US Mail, and the same rules cannot apply here.

BTW, the Andrew system here is not quite complete (despite what the wire

services may be saying), and the main convenience of the system is that its use is free, possibly because of the bugs. We have many other systems around that are MANY times faster, more secure, and more often even *working*, like the IBM 3083 ...

Re: Risks Involved in Campus Network-building

Don Wegeng <Wegeng.Henr@Xerox.COM>
5 Jan 87 17:30:20 EST (Monday)

I agree with Rich Kulawiec that a campus wide LAN is certainly subject to a large number of potential security risks, but it seems to me that such risks are present in any open computing environment. If an instructor keeps a draft of an exam online, but does not read protect the file, then any knowledgeable student with access to the system is capable of making a copy of the exam. There are similar risks associated with print spools, mail files, etc.

The presence of an LAN may make it difficult to detect some kinds of security violations, but this isn't a new problem. Any computer communications link that passes through uncontrolled space is subject to the same kinds of risks as a campus network. The technology exists to protect such links. I do not know whether the implementors of campus networks have made use of this technology, but it's certainly a reasonable question to ask.

Don

Risks Involved in Campus Network-building

<hplabs!pyramid!utzoo!henry@ucbvax.Berkeley.EDU>
Tue, 6 Jan 87 16:53:46 pst

It can get worse. Consider someone who is angry at the administration, perhaps having just flunked out, been expelled, or whatever. There is some sophistication involved in doing things like watching the network for passwords etc. There is little or no sophistication needed to just run some copper between the network cable and a 110V wall socket. Not only does this disrupt the network, it probably destroys a great deal of equipment, and creates a serious safety hazard. Good luck identifying the culprit, too! In most networking setups this would probably be utterly untraceable once the connection was broken.

I see reason for worry about newer, cheaper local-networking schemes that tend to run the network cable itself onto a board on each computer's backplane. Traditional thick-wire Ethernet is costly, but its transceivers do provide thousands of volts of isolation between network and computer. A disastrous fault on the network will only destroy transceivers. Fiber networks likewise provide inherent isolation.

The same problem exists, on a more modest scale, with existing setups involving RS232 cables. There the wiring is (probably) not a shared

resource, but the electronics on the other end are. If your computer facility casually runs RS232 cabling all over the building (as we do), remember that this means your computer is plugged into a net of wire with exposed pins in all kinds of places. RS232 interfaces are seldom opto-isolated, which is what would be needed to defend against electrical flaws in such setups.

That net of wiring also makes a dandy lightning antenna. That's one reason, by the way, why a separate-box modem is almost always a better idea than one that plugs into a backplane slot -- more isolation between phone line and computer.

Henry Spencer @ U of Toronto Zoology
{allegra,ihnp4,decvax,pyramid}!utzoo!henry

[Thanks. Enough on this topic for now? We seem to have plateued. PGN]

Engineering Ethics

Chuck Youman <m14817@mitre.ARPA>
Fri, 02 Jan 87 11:47:56 -0500

The December 28 op-ed section of the Washington Post included an article titled "The Slippery Ethics of Engineering" written by Taft H. Broome, Jr. He is director of the Large Space Structures Institute at Howard University and chairman of the ethics committee of the American Association of Engineering Societies. The article is too long to include in its entirety. Some excerpts from the article follow:

> Until now, engineers would have been judged wicked or demented if they were discovered blantantly ignoring the philosopher Cicero's 2,000-year-old imperative: In whatever you build, "the safety of the public shall be the highest law."
>
> Today, however, the Ford Pinto, Three-Mile Island, Bhopal, the Challenger, Chernobyl and other technological horror stories tell of a cancer growing on our values. These engineering disasters are the results of willful actions. Yet these actions are generally not seen by engineers as being morally wrong. . . Some engineers now espouse a morality that explicitly rejects the notion that they have as their prime responsibility the maintenance of public safety.
>
> Debate on this issue rages in the open literature, in the courts, at public meetings and in private conversations. . . This debate is largely over four moral codes--Cicero's placement of the public welfare as of paramount importance, and three rival points of view.
>
> Significantly, the most defensible moral position in opposition to Cicero is based on revolutionary ideas about what engineering is. It assumes that engineering is always an experiment involving the public as human subjects. This new view suggests that engineering always oversteps the limits of science. Decisions are always made with insufficient scientific information.

In this view, risks taken by people who depend on engineers are not merely the risks over some error of scientific principle. More important and inevitable is the risk that the engineer, confronted with a totally novel technological problem, will incorrectly intuit which precedent that worked in the past can be successfully applied at this time.

Most of the codes of ethics adopted by engineering professional societies agree with Cicero that "the engineer shall hold paramount the health, safety and welfare of the public in the performance of his professional duties."

But undermining it is the conviction of virtually every engineer that totally risk-free engineering can never be achieved. So the health and welfare of the public can never be completely assured. This gets to be a real problem when lawyers start representing victims of technological accidents. They tend to say that if an accident of any kind occurred, then Cicero's code demanding that public safety come first was, by definition, defiled, despite the fact that such perfection is impossible in engineering.

A noteworthy exception to engineer's reverence for Cicero's code is that of the Institute of Electrical and Electronics Engineers (IEEE)--the largest of the engineering professional societies. Their code includes Cicero's, but it adds three other imperitives opposing him--without giving a way to resolve conflicts between these four paths.

The first imperative challenging the public-safety-first approach is called the "contractarian" code. Its advocates point that contracts actually exist on paper between engineers and their employers or clients. They deny that any such contract exists--implied or explicit--between them and the public. They argue that notions of "social" contracts are abstract, arbitrary and absent of authority.

[The second imperative is called] the "personal-judgment" imperative. Its advocates hold that in a free society such as ours, the interests of business and government are always compatible with, or do not conflict with, the interests of the public. There is only the illusion of such conflicts. . . owing to the egoistic efforts of:

-Self-interest groups (e.g. environmentalists, recreationalists);

-The few business or government persons who act unlawfully in their own interests without the knowledge and consent of business and government; and

-Reactionaries impassioned by the loss of loved ones or property due to business-related accidents.

The third rival to public-safety-first morality is the one that follows from the new ideas about the fundamental nature of engineering. And they are lethal to Cicero's moral agenda and its two other competitors.

Science consists of theories for claiming knowledge about the physical world. Applied science consists of theories for adapting this knowledge to individual practical problems. Engineering, however, consists of theories for changing the physical world before all relevant scientific facts are in.

Some call it sophisticated guesswork. Engineers would honor it with a capitalization and formally call it "Intuition." . . . It is grounded in the practical work of millenia, discovering which bridges continue to stand, and which buildings. They find it so compelling that they rally around its complex principles, and totally rely on it to give them confidence about what they can achieve.

This practice of using Intuition leads to the conclusion put forward by Mike Martin and Roland Schinzinger in their 1983 book "Ethics in Engineering": that engineering is an experiment involving the public as human subjects.

This is not a metaphor for engineering. It is a definition for engineering.

Martin and Schinzinger use it to conclude that moral relationships between engineers and the public should be of the informed-consent variety enjoyed by some physicians and their patients. In this moral model, engineers would acknowledge to their customers that they do not know everything. They would give the public their best estimate of the benefits of their proposed projects, and the dangers. And if the public agreed, and the engineers performed honorably and without malpractice, even if they failed, the public would not hold them at fault.

However, most engineers regard the public as insufficiently informed about engineering Intuition--and lacking the will to become so informed--to assume responsibility for technology in partnership with engineers (or anyone else). They are content to let the public continue to delude itself into thinking that engineering is an exact science, or loyal to the principles of the conventional sciences (i.e., physics, chemistry).

Charles Youman (youman@mitre)

Search RISKS using swish-e

Report problems with the web pages to the maintainer

Search RISKS using swish-e

THE RISKS DIGEST

Forum on Risks to the Public in Computers and Related Systems

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

Volume 4: Issue 37

Wednesday, 7 January 1987

Contents

Re: vulnerability of campus LANs

<TMPLee@DOCKMASTER.ARPA>
Wed, 7 Jan 87 00:03 EST

Unless they're encrypted, of course they'll be busted wide open. I can remember in the late 60's the very first thing science or engineering students did at MIT and Harvard once they found out about the telephone tie lines was to see how far they could get (legally.) (you see, from Harvard you could get to MIT, from MIT to Mitre Bedford, from there to Washington, ...) (what got the freshman all excited was strange numbers that only answered "extension 55" or just "Yes?") (And I'm not talking about the blue-boxers either, which was big at the same time.) The mentality certainly hasn't changed ...

Risks Involved in Campus Network-building

David Fetrow <fetrow@entropy.ms.washington.edu>
Wed, 7 Jan 87 01:09:58 PST

From: "Wombat" <rsk@j.cc.purdue.edu>
> Imagine a university campus utilizing local area networking in academic
> buildings, dormitories, and other locations. Now picture someone with a
> reasonable aptitude for understanding the principles of LANs, and with
> motivation to subvert the campus LAN...and whose dorm room contains a wall
> socket marked "Southwest Campus Ethernet".

This particular scenario is partly avoidable by segmentizing the network: Using Bridges to isolate sections of the cable so that packets that don't need to be show up on the "dorm" cable, don't. (The Bridges must be secure of course). This at least removes the temptation of ultra-casual attacks.

Networking the campus may be "premature", in the sense we are courting a certain amount of disaster and we know it. We also know we need a lot more bandwidth than RS-232 can provide. In this case perhaps the right strategy isn't so much trying to prevent disaster but preparing for it. We've been here before (the easily cracked operating systems of the mid-70s'). The way secure (relatively) systems happened was by learning how their non-secure predecessors were attacked and fixing the holes just a little faster than 90% of the attackers found them.

-Dave "Very Worried" Fetrow-

Re: DES cracked?

<hplabs!pyramid!utzoo!henry@ucbvax.Berkeley.EDU>
Tue, 6 Jan 87 16:51:35 pst

Rumor hath it that the Videocypher II cracking exploited defects in the key-management scheme rather than a successful cryptanalysis of full DES.

> Second disclaimer: as the Radio-Electronics article points out, it's
> horrendously illegal to own or use any piece of equipment that "tampers with
> DES or attempts to profit from decoding it" (the article suggests that such
> action would be legally equivalent to treason, as DES is/may be under the
> protection of the NSA until 4/22/87)...

As has been discussed at some length in sci.crypt, this is utter nonsense. There is nothing illegal about breaking DES in your back yard, although there are various possible illegalities involved in *using* a DES-breaker for purposes like watching encrypted TV. DES is not under NSA's protection, and never has been. The R-E article notwithstanding, the US government does not use DES for its own communications. And the claim of treason is ludicrous: treason requires open aid to the US's enemies, including at least one overt act with multiple eyewitnesses. Being convicted of treason for anything less is literally unconstitutional -- the US Constitution itself defines treason to require these things. M/A-Com is just trying to scare people.

Henry Spencer @ U of Toronto Zoology
{allegra,ihnp4,decvax,pyramid}!utzoo!henry

Cellular risks

<Neumann@CSL.SRI.COM>
6 Jan 1987 13:37-PST

A long time ago Geoff Goodfellow reported on the ease with which one could spoof the cellular billing. Here is a more recent comment from him. (GEOFF@CSL.SRI.COM)

> Fraud and spoofing seem to be on the rise in cellular,
> with one carrier reportedly suffering at the rate of $180K/mo.

"Letters From a Deadman"

<Hoffman.es@Xerox.COM>
7 Jan 87 12:49:05 PST (Wednesday)

According to an article by Howard Rosenberg in today's 'Los Angeles Times', "Letters From a Deadman" is a Soviet-made movie about a nuclear holocaust triggered by a critical computer error. Dubbed in English, the 85-minute film is scheduled to air Feb. 12, on WTBS, Ted Turner's Atlanta-based cable super-station. From the article:

> The movie's central character is a man named Larsen, who is initially seen writing to his dead son from an underground bunker. Larsen is the scientist who developed the computers whose error triggered a devastating missile exchange that destroyed his family and country. Whatever country that is.
>
> "It's set in Western Europe, " said Martin Killeen, the WTBS producer on the movie project. "It could just as easily be Eastern Europe.... Having it set in a Western country, I think, allows the film makers more freedom. Obviously, in the Soviet mind, this [making a mistake that causes nuclear holocaust] is not something they would do. I just can't see them doing a story about a computer error if it were in the Soviet Union."

-- Rodney Hoffman

Stock Market Volatility

Randall Davis <DAVIS%OZ.AI.MIT.EDU@XX.LCS.MIT.EDU>
Wed 7 Jan 87 12:23-EST

Add to the risks of computers the danger of wider and faster dissemination of

misinformation (or at least incomplete information): several postings in the last few months have considered whether computerized stock trading might be causing the wild volatility seen in the market recently. But no one seems to have asked an important question: was there in fact any markedly higher volatility. The answer may in fact be no.

The December 86 issue of Money has an interesting 1-page article with a graph of stock market volatility, measured as "annualized monthly standard deviation of the S&P 500", and there's the key issue: how to measure it. On their standard, the highest period is a clear peak around 1937, with lesser peaks around '62, '70, and '74. Since programmed trading began (in 1982, despite all the newspaper articles that make it appear to have been invented yesterday), volatility has in fact DIMINISHED and has only recently begun to head upward again toward the level of the (smaller) '62 and '70 peaks.

Their interesting claim is that with programmed trading

> "... there is a risk that an innocuous market downturn may be greatly magnified. So far, however, programmed trading has proved to have few lingering effects on stocks. It can compress a market movement that would otherwise take a day -- or even a week -- into a period as short as 10 minutes. But if a market move would not otherwise have occurred, it is likely to reverse itself within a few days.... while the market's volatility is a bit higher this year than it has been in the past three years, it remains quite normal by historical standards."

Note in particular the last seven words.

I am neither economist enough nor statistician enough to judge whether their metric is appropriate, but there are several important overall issues here:

1) The issue requires non-trivial economic and statistical sophistication. The half-assed analyses widely quoted are appallingly naive in part because they never even question whether the issue may be deeper than watching the daily averages and seeing meaningless records set.

2) The media in general want NEWS, something dramatic that has never happened in the history of the universe and that may in the next 18 seconds lead to the collapse of civilization. The story is even better if it involves something that a large number of people find inherently threatening, and technology -- particularly computer-related -- is a favorite candidate (nuclear energy, gene splicing and various diseases rank up there pretty high too). All this, plus the press of time to get to press lead to two serious faults:

a) not asking the obvious questions: "Has this happened before; is it really unusual" Often the answers are yes, and no, respectively. But what a boring story that would make.

B) not questioning the premises: the market drop of 86 points on September 11 was the LARGEST IS HISTORY, omigod! Yes, but it was only the third largest in terms of percentage. And what's the right measure anyway? Absolute points, percentages? And why 1 day? What's sacred about the market's performance over a 1-day trading cycle? Why not a week or a month or a year or a business

cycle? Why doesn't anyone worry about the biggest 1-hour drop on record or the biggest 10 minute decline? What is the relevant metric? Is the alleged phenomenon even real?

3) Our agenda in RISKS should be to debunk, not contribute to misinformation. Where our technical skills are relevant, we can do that particularly well. Where they are not (as in the need here for economic and statistical savvy), we should tread quite carefully. We too need to remember to question the assumptions.

4) There's risk in incorrect and incomplete information; there's computer-related risk when that information is widely disseminated electronically:
the British telephone billing scam that apparently wasn't;
the automated bibliographic retrieval system that required keywords in the article title (only it didn't);
more recently the illegal cracking of DES that wasn't illegal and didn't happen;
and perhaps the stock market volatility that isn't.
We should be particularly aware of this misinformation risk since it is entirely under our control.

Engineering ethics

Dick Karpinski <dick@cca.ucsf.edu>
Wed, 7 Jan 87 17:43:36 PST

Cicero's rule notwithstanding, there are many cases of opposition twixt risks of doing versus risks of not doing. I recall, for example, that our H.J. Kaiser offered to build troop carriers rather quickly using rivets instead of welded seams. I'm too young to remember whether his offer was accepted, but it seems clear that he was not denounced for being prepared to make less seaworthy ships, which therefor increased the risks of loss of life during troop transport. The alternative was increased risks of loss of life at the front lines of WWII.

I am prepared to accept a dollar value on human life in order to discuss these decisions in reasonable ways. Many, even most, people are not so prepared and would consider me to be a barbarian beast on just those grounds. Perhaps it will be necessary to do some heavy duty education (of which side?) before consensus can be reached. Incidentally, my guess is that currently, we should value one human life somewhere between $100k and $1m. The risks of failing to do so are in the nature of making the necessary choices on arbitrary or irrational grounds, or in hiding the decision entirely from view (and finding scapegoats as needed).

Dick Karpinski Manager of Unix Services, UCSF Computer Center
UUCP: ...!ucbvax!ucsfcgl!cca.ucsf!dick (415) 476-4529 (11-7)
BITNET: dick@ucsfcca Compuserve: 70215,1277 Telemail: RKarpinski
USPS: U-76 UCSF, San Francisco, CA 94143-0704

Computerized Discrimination

Ken Laws <LAWS@SRI-IU.ARPA>
Wed 7 Jan 87 15:54:13-PST

I just caught up with the Risks discussion and noticed two messages on computerized discrimination against women and blacks applying to a medical school. Randall Davis made the implicit assumption that the discrimination consisted of a rule subtracting some number of points for sex and race, and questioned whether the programmer shouldn't have blown the whistle.

I think it much more likely that the decision function was a regression equation that happened to include coefficients combining sex and race with other predictor variables. The programmer -- or statistician, probably -- would have done this out of carelessness or simply to obtain the best possible fit to the admissions decisions in the database. The school administration would have accepted the formula as valid, probably without even examining it, if it correctly classified the past applicants and performed reasonably on the new ones. I'm not too surprised that no one paid attention to the sign or magnitude of the coefficients.

So much for the mechanism of this computer (or statistical) risk. Now I'd like to put in a few words in defense of the statistical approach.

Suppose you had to screen equal numbers of male and female applicants and you wanted to admit them equally. Suppose further that women tended to have higher verbal scores. If you used only these scores, too many women would be admitted. It would be necessary for you to balance the high scores, either by subtracting something for being female or by boosting the coefficient for some male-dominated variable (e.g., math scores). This type of twiddling is exactly what a regression program does. It selects whichever adjustment (or combination of adjustments) gives the best fit. The program could produce exactly the same results, or discrimination, even if you forced it to use <>positive<< coefficients for female and black codes.

I'm not suggesting that the school's formula was a good one. They should have ignored sex and race unless they intended to set quotas. By matching a database of past decisions they were undoubtedly freezing any biases that had existed in the past; perhaps the formula recorded these biases accurately.

I am suggesting that the individual coefficients in a regression formula have little meaning unless you consider all of the intercorrelations and do a proper sensitivity analysis.
The article said that this school had a good admissions record, so people shouldn't be hasty in putting them down. Let he who fully understands his own database cast the first stone.

Also: statistical tools are powerful in the right hands, dangerous in the wrong ones. Don't assume that you can do a regression just because your micro can do one. If your data is worth being analyzed, it is probably worth being analyzed by a professional. And if you

really want good results, work with the professional from the start instead of collecting the data and mailing it in for an analysis.

-- Ken Laws

Search RISKS using swish-e

THE RISKS DIGEST

Forum on Risks to the Public in Computers and Related Systems

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

Volume 4: Issue 38

Thursday, 8 January 1987

Contents

As the year turns ...

Jeffrey Mogul <mogul@decwrl.DEC.COM>
8 Jan 1987 1846-PST (Thursday)

A number of sites, including my own, have special receivers for the time signal transmitted by the GOES satellite; the time information comes from the National Bureau of Standards, and with a properly adjusted setup you can set your computer's clock to with a few milliseconds. Since the clocks are somewhat expensive, many hosts instead slave their clocks to one of the hosts endowed with its own satellite receiver.

The data stream from the NBS tells you what time of day it is, and what day of the year it is, but it does not say what year it is. The usual practice is to assume that the local host knows what year it is, and to get the correct time you combine the satellite clock's time-within-year with your

local knowledge of the year.

Needless to say, this doesn't quite always work. Mostly, it tends to not work on New Year's Eve, when many of us would rather not be fixing our computers. Dave Mills does a great job keeping a bunch of clocks running, on which many other hosts on the Internet depend. This is his message from early on January 1st:

> From: mills@huey.udel.edu
> Subject: Ask not for whom the chimes tinkle
> To: tcp-ip@sri-nic.arpa, nsfnet@sh.cs.net
>
> Folks, Every year it's the same - I forget UT midnight comes five hours before the ball drops in Times Square. For an hour and sixteen minutes after the hoot and holler in Trafalgar Square at least four radiofuzz timetellers still squawked yesteryear. DCN1, UMD1, FORD1 and NCAR springs have now been rewound to 1987 and all you guys can forget those whopping disk-usage refunds. Thanks to Hans-Werner Braun, who reminded me of my annual first duty of the new year and annual first resolution to figure out how to avoid paw to keyboard in the absence throughout the world, as far I know, of a highly reliable electronic way to find out what year it is.

It turns out that as recently as today, several Internet sites are still stuck in 1986, apparently as a result of the efficient distribution of faulty time information.

Meanwhile, I thought I had foreseen all eventualities and fixed the program used here at DECWRL, so that as the year turned it would avoid becoming confused. The important thing is to be sure not to try to set the time during a period where the satellite clock thinks it is one year and the local clock thinks it is a different year. Needless to say, I got this part wrong, and our clocks promptly jumped ahead exactly one year. I found at least two bugs in my code, but I still don't completely understand what went wrong, and I'm sure something is going to go wrong again next year.

I guess the lesson is that it is wrong to assume that the least significant bits are the hardest to get right. (One reader of TCP-IP told of how he had to use a similar year-less time format when designing a missile-tracking system 20 years ago, and had to put in special logic to be sure that the system could survive the confusion on New Year's Eve.) Now, if I could only make it through January without writing "1986" on any checks.

Automobile micros

<Murray.pa@Xerox.COM>
Thu, 8 Jan 87 12:31:37 PST

Our hero, Joe, works for one of the "big 3" automakers near Detroit, that strange corner of the US where everybody a late model American car. One day, Joe was calmly driving down the highway, accelerating gently, when his car

stuttered a bit. It wasn't a big deal. Most people probably wouldn't have noticed it. However, Joe's job was programming the small computer that controls the gas and timing for car engines, so he this behavior caught his attention.

When Joe got to work, he popped the cover off the computer in his car and took the main chip into the lab. After a bit of work, he managed to reconstruct the necessary input conditions, and sure enough the glitch was real. Happy that he had tracked down a minor problem in has car, Joe prowled around the lab for replacement chip. It didn't take long to find one.

Rather than just installing the new chip in his car, Joe decided to try it in his test rig. You guessed it, the "good" chip had the same problem. So did several others - all the ones he found to try.

The story ended there. My guess was a PROM bug, but I didn't get that from the horses mouth.

Speaking of risks, the first time that GM does a major recall because of software is going to get a lot of publicity. I'll bet much of it will be mud for the computer profession rather than teaching the public about the realities and economics of software.

Chemicals in semiconductor manufacturing

Michael Scott <scott@rochester.arpa>
Thu, 8 Jan 87 15:12:22 est

Several submissions recently have concerned the risks of miscarriages and other health problems associated with semiconductor manufacturing. For anyone interested in the subject, I highly recommend the cover story of the October 1985 issue of the Progressive magazine: "Dead End in Silicon Valley" by Diana Hembree. Where recent attention has focussed on IC fabrication, the Progressive article is mainly about PC board assembly, where low-paid semi-skilled workers, mostly women, are reportedly exposed to large numbers of toxic, allergenic, and carcinogenic chemicals, with a shocking array of side effects. To obtain background information, Hembree took a job for four months as an assembler at Q.E.S. Corp. in Santa Cruz. Her story makes pretty grim reading.

Re: re: Cellular -- Ref to Geoff

Peter G. Neumann <Neumann@CSL.SRI.COM>
Thu 8 Jan 87 11:28:30-PST

I had several queries about how could one possibly spoof the cellular phone system? Some of you will recall the earlier contribution from Geoff Goodfellow in RISKS-3.10 noting that it is indeed utterly trivial to change your ID.

"Misinformation"??

Dick Karpinski <dick@ccb.ucsf.edu>
Thu, 8 Jan 87 17:24:30 PST

In RISKS DIGEST 4.37
Stock Market Volatility (Randall Davis)

>Date: Wed 7 Jan 87 12:23-EST
>From: Randall Davis <DAVIS%OZ.AI.MIT.EDU@XX.LCS.MIT.EDU>
>...
>4) There's risk in incorrect and incomplete information; there's
>computer-related risk when that information is widely disseminated
>electronically:
> the British telephone billing scam that apparently wasn't;
> the automated bibliographic retrieval system that required keywords
> in the article title (only it didn't);
> ...
>We should be particularly aware of this misinformation risk since it is
>entirely under our control.

I don't recall being satisfied that there was no British phone scam.
What was it that convinced you?

[It is altogether possible that BT is covering up. On the other hand, their description of the system (by phone, to me) stated that the READ-AFTER-WRITE check is properly implemented and that there are three other checks as well. They claim that the Sunday Post will print a retraction. (As yet no one has reported seeing it.) Of course, there may be still be other vulnerabilities. RISKS readers are learning to look the proverbial gift horse in the mouth, as well as the horse you had to pay a fortune for. PGN]

The bibliographic retrieval system is worse that had been alleged in the 29 Sep 86 Risks 3.70. It is not a "new policy" according to one Paul Ryan of the DTIC in 4.23, but a limitation of their software. But the fact is that only the first five words (including articles and prepositions) of titles are involved in automatic searches. This strikes me as an unconsciencable restriction to be removed as soon as practicable. I would certainly hesitate to count on such a system. For example, Parnas' seminal CACM article on modularity ("On the Criteria to be Used in Decomposing Systems into Modules") would only show up in searches for "On", "the", "Criteria", "to", and "be". What a travesty of search, retrieve, and help!

["To be or not to be..." would show up even more dramatically! PGN]

"We should be particularly aware of this misinformation risk since it is entirely under our control."

How can I offer to help these poor souls correct (improve) their shabby software? How else but by discussing these problems can we become informed about the sad existing conditions?

Dick Karpinski Manager of Unix Services, UCSF Computer Center
UUCP: ...!ucbvax!ucsfcgl!cca.ucsf!dick (415) 476-4529 (11-7)
BITNET: dick@ucsfcca or dick@ucsfvm Compuserve: 70215,1277
USPS: U-76 UCSF, San Francisco, CA 94143-0704 Telemail: RKarpinski

Burnham Book -- A Recommendation

Alan Wexelblat <wex@mcc.com>
Thu, 8 Jan 87 10:40:59 CST

Some time ago, Dave Taylor (on mod.comp-soc) recommended a book called "The Rise of the Computer State" by David Burnham. I have purchased this book and hereby recommend it to RISKS readers. Burnham is an investigative reporter, so the book tends to have a bit of a sensationalistic streak, but it is very interesting and covers many topics of interest to RISKS readers. The edition I have is softcover, published in 1984 by Vintage books for $6.95. It's ISBN 0-394-72375-9.

People like PGN who collect RISKS-anecdotes may be interested in some of the stories he tells (like the part played by punch-cards in the 1942 roundup of Japanese-Americans).

Alan Wexelblat
ARPA: WEX@MCC.ARPA or WEX@MCC.COM
UUCP: {seismo, harvard, gatech, pyramid, &c.}!ut-sally!im4u!milano!wex

Engineering Ethics

ball@mitre.ARPA <Dan Ball>
Thu, 08 Jan 87 11:29:37 -0500

The discussions concerning engineering ethics in RISKS 4.36 and 4.37 overlook what I think is a far more critical contributor to modern engineering disasters than the personal ethics (or lack thereof) of individual engineers: the organizational environment in which engineers must function.

Large engineering projects involve many thousands of engineers, and the time required to complete them has stretched, in many cases, to over twenty years. In this environment, it can be difficult for an individual to feel any personal responsibility for the outcome of the overall project. Most of the engineers I know are neither "demented" nor "morally wicked." They are just trying to do their job in the midst of a bureaucracy where authority is diffused and decisions are made by committee. It is to be expected that short-term expediency will usually prevail, particularly when it is difficult or impossible to assess the long-term consequences of a decision.

The organizational dynamics involved in the development and operation of safety-critical systems and their effect on the individuals concerned are submit, far more important than the contemplation of Cicero's ethics.

Although I don't consider Dick Karpinski a "barbarian beast", I question whether assigning a monetary value to human life would provide additional insight into the management of risks. I am not convinced that we know how to predict risks, particularly unlikely ones, with any degree of confidence. I would hate to see a $500K engineering change traded off against a loss of 400 lives @ $1M with a 10E-9 expected probability. I'm afraid reducing the problem to dollars could tend to obsure the real issues.

Moreover, even if the analyses were performed correctly, the results could be socially unacceptable. I suspect that in the case of a spacecraft, or even a military aircraft, the monetary value of the crew's lives would be insignificant in comparison with other program costs, even with a relatively high hazard probability. In the case of automobile recalls, where the sample size is much larger, the manufacturers may already be trading off the cost of a recall against the expected cost of resulting lawsuits, although I hope not.

Clearly, though, those of us concerned with safety need to find some way of seeing that risks are effectively managed in large projects. It is not enough to act as a perpetual doomsayer standing in the way of progress. To be effective, safety engineers must be perceived as helpful and participate in the mainstream of the design activity.

Re: Stock Market Volatility

Richard A. Cowan <COWAN@XX.LCS.MIT.EDU>
Thu 8 Jan 87 20:31:27-EST

Randall Davis makes the important point that stock market trading really isn't any more volatile now than before. I agree.

Computers have enabled the VOLUME of trading to go up (probably to a level where much of the speculation serves no useful economic purpose to non-speculators), but this does not seem to automatically insure stock market volatility. Even if computerized trading becomes more widespread, I would think that any aberrant trades would be quickly corrected the next day as long there remains some human input into the trading process. Yet I still see a potential effect.

A book I once read on the Stock Market crash of 1929 noted that in times of potential panic, large traders would attempt to shore up the market by buying, to restore confidence in the market. It's possible that the stability of the present market has a lot to do with this type of activity. But such "feedback" -- applied by large banks and brokerage firms -- would not in the foreseeable future be applied automatically by computer, because the decisions involve analyzing political events and the psychological mood "on the Street."

If there currently exists a human rudder smoothing the path of the stock market, I can see why investors might be concerned about

programmed trading. This practice does not run the risk of a computerized avalanche of domino trades which will drive the market 1000 points up or down in one day. But it may interfere with the ability of large investors to use their resources as a rudder, in the event that trading does become volatile for economic reasons.

It is easy to see why the programmed trades get media attention. On the "triple-witching-hour" days, human beings will have less control and the market may do unexpected things. If these events are not announced and explained before they occur, the movement of the market may set off an avalanche of HUMAN panic selling. Of course, this would only occur if the preconditions existed were met -- if the market were viewed to be overvalued, relative to economic performance.

It is true that the news media sensationalizes and often fails to put stories into historical context; they may seem to enjoy blaming technology. But consider the motivations of the people from whom the business press usually get their stories: people in the financial community. They may find technology a convenient scapegoat for any problem with the stock market, especially if they have contributed to setting up the conditions of an overvalued market.

Perhaps the market hasn't reached the point where it is overvalued. But consider that the head of the MIT Department of Electrical Engineering and Computer Science, in an open forum on US competitiveness with Japan last February, said "I think we're going to have a depression."

Lester Thurow and several other economists are now making frequent comparisons to 1929, pointing out when large investors finally lost confidence in the ability of the market to sustain a continued rally or plateau, they all raced to pull out. Anyway, the point is that computers will not cause a crash, but could set off a crash that is bound to occur anyway, and be wrongly blamed for it.

Of course, it is possible that there might not be a crash at all! When US investors sell, foreign investors will buy up all our stock and we'll be owned by the Japanese! :)

-rich

Search RISKS using swish-e

Search RISKS using swish-e

THE RISKS DIGEST

Forum on Risks to the Public in Computers and Related Systems

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

Volume 4: Issue 39

Sunday, 11 January 1987

Contents

Re: As the year turns ... (Jeffrey Mogul)

Jerome H. Saltzer <Saltzer@ATHENA.MIT.EDU>
Fri, 9 Jan 87 12:40:24 EST

I believe it was New Year's eve, 1962, when I first found myself poking around inside a system--M.I.T.'s Compatible Time-Sharing System for the IBM 709--that was nominally intended for continuous operation, but that had to be *recompiled* to tell it about the new year, because whoever designed the hardware calendar clock assumed that someone (else) could program around the missing year field.

It took only a small amount of contemplation to conclude that any source that claims to tell you the date has got to mention the year, and with some browbeating of engineers we got a version of that design included in the Multics hardware a few years later.

At the time, someone talked me out of writing a paper on the subject on the basis that the right way to do it is so obvious that noone would ever be so dumb as to design a date-supplying clock without the year again. Possible conclusion for RISKS readers?: nothing, no matter how obvious, is obvious.

Jerry

911 computer failure

Peter G. Neumann <Neumann@CSL.SRI.COM>
Sat 10 Jan 87 12:04:00-PST

From an article by Dave Farrell, San Francisco Chronicle, 9 Jan 1987:

The city's failure to send help to a choking 5-year-old boy was attributed to equipment failure, not human error, according to Mayor Dianne Feinstein. When Gregory Lee began choking, his Cantonese-speaking grandmother dialed 911, but gave up when no one understood her. The automatic call-tracing program somehow retrieved the wrong address and displayed it on the police controller's computer screen. (The rescue crew was directed to the wrong address.)

Engineering tradeoffs and ethics

Andy Freeman <ANDY@Sushi.Stanford.EDU>
Fri 9 Jan 87 09:58:41-PST

Dan Ball <Ball@mitre.ARPA> wrote: [He mentions that many engineering organizations are so large and projects take so long that individual responsibility is suspect and the uncertainty in predicting risks.]
I'm afraid reducing the problem to dollars could tend to obsure the real issues.

What issue is obscured by ignoring information?

> Moreover, even if the [cost-benefit] analyses were performed correctly, the results could be socially unacceptable. [...] In the case of automobile recalls, where the sample size is much larger, the manufacturers may already be trading off the cost of a recall against the expected cost of resulting lawsuits, although I hope not.

Between legal requirements and practical considerations (they can't pay out more than they take in), manufacturers MUST trade off the cost of a recall and other legal expenses against costs and probability.

The result of a cost-benefit/risks analysis is information, not a decision. This information can be used to make a decison. I think it is immoral for a decision maker to ignore, or worse yet, not determine cost-benefit or other relevant information. (There is a meta-problem. How much should gathering the information cost? People die while drugs undergo final FDA testing. Is this acceptable?) In addition, gathering the information necessary to determine it often finds opportunities that the decision maker was unaware of.

Since we'd like to have cars, there will always be some safety feature that is unavailable because we can't afford a car that includes it. (Because autos and "accidents" are so common, auto risks can be predicted fairly

accurately.) Unfortunately, the current legal system restricts our access to information about the tradeoffs that have been made for us. You might buy a safer car than I would, but you don't have that information. The costs are spread over groups that are too diverse. A legal system that encourages that is socially unacceptable.

-andy

Engineering Ethics

Ken Laws <LAWS@SRI-IU.ARPA>
Fri 9 Jan 87 10:15:26-PST

> Date: Thu, 08 Jan 87 11:29:37 -0500 <RISKS-4.38>
> From: ball@mitre.ARPA <Dan Ball>
>
> ... I am not convinced that we know
> how to predict risks, particularly unlikely ones, with any degree of
> confidence.

True, but that can be treated by a fudge factor on the risk (due to the risk of incorrectly estimating the risk). There are difficulties, of course: we may be off by several orders of magnitude, different tradeoffs are required for large, unlikely disasters than for small, likely ones, and certain disasters (e.g., nuclear winter, thalidomide) may be so unthinkable that a policy of utmost dedication to removing every conceivable risk makes more sense than one of mathematically manipulating whatever risk currently exists.

> I would hate to see a $500K engineering change traded off against
> a loss of 400 lives @ $1M with a 10E-9 expected probability. I'm afraid
> reducing the problem to dollars could tend to obsure the real issues.

How about a $500M tradeoff against a loss of 1 life with a 10E-30 probability? If so, as the punch line says, "We've already established what you are, we're just dickering over the price." The values of a human life that are commonly accepted in different industries seem to fall in the $1M to $8M range, with something around $2M being near the "median".

> Moreover, even if the analyses were performed correctly, the results could
> be socially unacceptable. I suspect that in the case of a spacecraft, or
> even a military aircraft, the monetary value of the crew's lives would
> be insignificant in comparison with other program costs, even with a
> relatively high hazard probability.

The "value of a human life" is not a constant. The life of a volunteer or professional, expended in the line of duty, has always been considered less costly than the life of innocents. If we forget this, we end up with a few $60M fighter aircraft that can be shot down by two or three less-secure $5M aircraft. (I predict that the next protracted U.S. war will be won by expendable men in jeeps with bazookas, not by autonomous vehicles.)

> In the case of automobile recalls, where the sample size is much larger,
> the manufacturers may already be trading off the cost of a recall against
> the expected cost of resulting lawsuits, although I hope not.

Of course they are. The cost of lawsuits is much more real than any hypothetical cost of human life. In fact, the cost of lawsuits <>is<< the cost of human life under our current system. The fact that awards differ depending on manner of death, voluntarily assumed risk, projected lifetime income, family responsibilities, etc., is the reason that different industries use different dollar values.

I think we should set a formal value, or set of values, if only to ease the burden on our courts. It would give us a firm starting point, something that could be adjusted according to individual circumstance. This is already done by the insurance industry and their guidelines are also used by the courts in setting reasonable damage awards ($x for mental suffering, $y for dismemberment, ...). It would not be a big change to give legal status to such values. Courts would still be free to award punitive damages sufficient to inflict genuine influence on rogue corporations.

As for the dangers of incorrectly estimating risks, I think that the real danger is in not estimating risks.

-- Ken Laws

Engineering Ethics

George Erhart <gwe@cbosgd.mis.oh.att.com>
Fri, 9 Jan 87 16:05:50 est

Whether or not we like to admit it (or even are aware of it), we all (not just engineers) place a monetary value on human life. For example, consider the number of people who drive small cars; most of these are less survivable in a collision than larger, more expensive autos. The purchasers usually are aware of this, but accept the risks to save money.

How many of us have rushed out to have airbags installed in our cars ? How often do we have our brakes checked ? Do we even wear our seatbelts ?

The facts are that :
1)No system can be made 100% safe/infallible.
2)The cost of the system increases geometrically as the 100% mark is approached
3)A compromise *must* be reached between cost and safety.

A good example of the latter would be in the design of ambulances. We could make them safer via heavier construction, but this would decrease top speed (which also makes the vehicle safer). The increased response time, however, would endanger the lives of the patients. Larger engines can be installed to regain speed, increasing both the purchase cost and operating expense, which will result in fewer ambulances being available, and increased response time.

We set the value of human life in countless ways. We must; it is an unavoidable situation. But that value is rarely set by an engineer; it is fixed by the consumer (read you and me) who determine how much they are willing to pay for their own safety.

Bill Thacker - AT&T Network Systems, Columbus, Ohio

Re: computerized discrimination

Randall Davis <DAVIS%OZ.AI.MIT.EDU@XX.LCS.MIT.EDU>
Sun 11 Jan 87 13:54-EST

> Date: Wed 7 Jan 87 15:54:13-PST
> From: Ken Laws <LAWS@SRI-IU.ARPA>
> Subject: Computerized Discrimination
>
> ... Randall Davis made the implicit assumption that the discrimination
>consisted of a rule subtracting some number of points for sex and race,
>and questioned whether the programmer shouldn't have blown the whistle.

Here's the relevant paragraph:

> One can only imagine the reaction of the program authors when they discovered what one last small change to the program's scoring function was necessary to make it match the panel's results. It raises interesting questions of whistle-blowing.

There's no assumption there at all about the form the scoring function.

One "small change" that would be at the very least worth further investigation is the need to introduce race as a term. Whatever its coefficient, the need to introduce the term in order to match the human result should at least give one pause. That's the whistle-blowing part: one ought at least to be wary and probe deeper. "Reading the polynomial" to determine the direction of the effect may not be an easy task, but this is one situation where the circumstances should quite plausibly inspire the effort.

The point remains that the polynomial, once created, can be examined and tested objectively. No such option exists for people's opinions and unstated decision criteria.

Search RISKS using swish-e

Report problems with the web pages to the maintainer

Search RISKS using swish-e

THE RISKS DIGEST

Forum on Risks to the Public in Computers and Related Systems

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

Volume 4: Issue 40

Wednesday, 14 January 1987

Contents

Phone Cards

Brian Randell <brian%kelpie.newcastle.ac.uk@Cs.Ucl.AC.UK>
Wed, 14 Jan 87 16:12:23 gmt

PHONE CARDS - THE PLOT THICKENS

At PGN's implied request, I have tracked down, and talked to the Sunday Post reporter who wrote the original story on the phone card fraud. These notes of my telephone conversation with him are being sent to RISKS with his explicit permission, though he asked that his name not be included.

The Sunday Post was indeed asked by BT to publish a retraction, but have refused to do, though they have published a letter from BT expressing

(BT's) full confidence in the phone card system. Based on previous experiences - "we often get complaints at our stories" - the reporter regards the fact that BT did not push for a retraction, but instead merely settled for publication of their letter, as tantamount to an acceptance of the truth of the original story.

He claims to be still sure that the fraud is possible, and to have seen it being worked, at several different phones, by the soldiers, in the presence of several other witnesses. He does admit that he was himself later unable to demonstrate the fraud successfully to some BT engineers who travelled to Glasgow to meet him. He however has since talked to one of the soldiers, who assures him that the fraud is still working, but will not reveal to the reporter, leave alone BT, where he (the reporter) went wrong in trying to duplicate the method of fraud. (The other soldier - who did not want the original story published, because it would interfere with "free" international calls - is now refusing to talk to the reporter.) Moreover the reporter claims to have received a phone call from a BT engineer at Watford, confirming the practicability of the fraud.

Brian Randell - Computing Laboratory, University of Newcastle upon Tyne

ARPA : brian%cheviot.newcastle.ac.uk@cs.ucl.ac.uk
UUCP : <UK>!ukc!cheviot!brian
JANET : brian@uk.ac.newcastle.cheviot

It's No Joke!! (Microwave oven bakes 3 yrs of PC data)

"Lindsay F. Marshall" <lindsay%kelpie.newcastle.ac.uk@Cs.Ucl.AC.UK>
Tue, 13 Jan 87 09:58:03 gmt

There was a report on the wireless this morning that a well-known comedian lost 3 years worth of material stored on his home computer when his wife turned on the microwave oven!! Sadly, I have no more information than this as the papers have not arrived in Newcastle because of the weather.....

[Continued: Wed, 14 Jan 87 09:09:14 gmt]

The most detailed information about the incident I can find says that the comedian's son was playing with the machine in the kitchen when his mother turned on the microwave oven. The computer's "memory" was instantly wiped. The suggested reason is (of course) leakage from the microwave oven. The wife's comment? "I told him he shouldn't use the computer in the kitchen..."

Automation bottoms out

Peter G. Neumann <Neumann@CSL.SRI.COM>
Wed 14 Jan 87 10:27:58-PST

``As for the `partially shielded street urinals' of Paris ... they have been superseded by sexually neutral, fully enclosed, fully automated, coin-access two-stall elliptical masonry structures.... A few years

ago, a child was killed in one of them by the automated toilet seat.''

(Letter to the editor of the New York Times from Louis Marck, excerpted [exactly as shown] in the SF Chron, 13 Jan 87, p. 10)

Amtrak train crash with Conrail freight locomotive -- more

Peter G. Neumann <Neumann@CSL.SRI.COM>
Wed 14 Jan 87 10:34:53-PST

Tests conducted (three times) indicated that the freight locomotive should have been able to stop in time, and that equipment was all in working order. Thus human error was the most likely cause of the accident that killed 15 (13 Jan 87, SF Chron, p. 8, from the Washington Post). (Earlier reports suggested that three separate safety mechanisms would have had to fail at the same time [for it to have been other than human error].)

Re: Cellular risks

<Frankston@MIT-MULTICS.ARPA>
Tue, 13 Jan 87 00:01 EST

I picked up a book entitled "Introducing cellular communications: The New Mobile Telephone System" from TAB Books. The copyright is 1984. From the look of it, it seemed to be a lightweight book. Skimming it, it seems instead to go into details of message formats, setting up head ends and other detailed stuff. I presume it makes it much easier to figure out how to hack the system.

> [This is an old hack. As noted here before, the idea(l) is to make the system design strong enough that all the documentation (except maybe the vulnerability analyses) can be freely handed out. Of course, the reality is far from that ideal. PGN]

Re: Ask not for whom the chimes tinkle

<ihnp4!nears!ks@ucbvax.Berkeley.EDU>
Sat, 10 Jan 87 09:01:37 PST

In article <8701082340.AA17468@ucbvax.Berkeley.EDU> Perrine@LOGICON.ARPA (Tom Perrine) wrote:

> WARNING! TIME WARPS AHEAD!
>
> Well the chimes sure tinkled for us! On Thursday 8 Jan (1987 A.D.) at about 1400 PST we queried DCN1 as we booted our PWB UNIX system and received a 1986 date stamp! (Gee Mr. Peabody, set the Wayback machine for 1987!)

Further investigation shows that DCN6 and GW.UMICH.EDU are also stuck in a time warp. UMD1 seems to be the only un-nostalgic clock. (FORD1 was not reachable.)

For now, everyone better keep one eye on the Timex, and another on the packets, and another on the Seiko!

Tom Perrine, Logicon - OSD

Re: Engineering ethics

Peter G. Neumann <Neumann@CSL.SRI.COM>
Wed 14 Jan 87 19:22:11-PST

Sorry. It is time to blow the whistle on this rather narrowly focussed discussion. Sorry to those who thought they had more to say on the subject. (I tacked a comment on the Ford Pinto case onto Andy Freeman's note in RISKS-3.65 -- some of you will remember -- on how short-sighted dollar-values on lives can be.) PGN

Repetitive Strain Injury and VDTs

<MJackson.Wbst@Xerox.COM>
14 Jan 87 10:49:09 EST (Wednesday)

The January/February issue of the /Columbia Journalism Review/ contains an article entitled "A Newsroom Hazard Called RSI" about repetitive strain injury associated with workstation use. It is much too lengthy to reproduce, but attached below are some excerpts.

Mark

"[San Diego /Tribune/ reporter John] Furey is a victim of repetitive strain injury (RSI), a term that embraces a number of painful and often disabling afflictions linked to continuous bending, twisting, and flexing of the hands, arms, or shoulders. Thousands of these injuries, which include tendonitis, are found among meat-cutters, garment workers, and other workers whose jobs require constant, repeated hand movements. But repetitive strain injuries are also showing up among office workers, who may strike a computer keyboard up to 45,000 times an hour. And automated newspaper offices are no exception: to the dismay of all involved, disabling cases of RSI have recently cropped up in newspapers across the country."

. . . .

"Her doctor, John Adams, a Los Angeles orthopedist, compared her case of tendonitis to 'four tennis elbows,' [/Los Angeles Times/ reporter Penelope] McMillan recalls. 'He said he'd never seen anything like it.' Returning to work after a two-and-a-half-month leave, McMillan found that anti-inflammatory drugs had no effect on the recurrent 'wild' pain in her arms."

. . . .

"Steven Sauter, a job-stress specialist with the National Institute for Occupational Safety and Health, believes that VDT-related injuries are relatively uncommon. But, he warns, 'when these problems do occur, they can be serious and require medical attention.'

"One problem, Sauter notes, is that many VDT jobs 'have little built-in variety.' In a job-health manual he wrote while teaching at the University of Wisconsin, Sauter explained that VDT operators often make thousands of keystrokes an hour, 'repeating nearly identical motions at a high rate of speed.' While typing, each stroke requires muscles to contract and tendons to move, and the tendons can become irritated as they slide around bones and against tissues. In such cases, he warns, the wear and tear can cause painful inflammation of the tendons, which will not heal without rest."

. . . .

"Indeed, a question that puzzles many editors is why some employees who had no problems when they used typewriters are developing hand and arm injuries now that they are using VDTs. One answer, say occupational health specialists, is that, although some typists do develop such injuries, VDT users may be at greater risk because they can make many more hand movements per hour. In addition, using a typewriter calls for more varied hand movements and breaks in routine, such as inserting paper.

"Another factor that may contribute to injuries is that some reporters are simply using their VDTs /more/ than they used typewriters. 'At the /Times/, we used to do anything to avoid using our clunky old manual Olympics,' [/Los Angeles Times/ reporter Laurie] Becklund says. 'We'd take notes by hand--anything. When we got VDTs, we were thrilled. They were so convenient that we began using them for everything.'"

. . . .

"For Becklund, who receives physical therapy for her hands three times a week, the worst is not knowing when her hands will be healed. 'It's hard not to feel depressed, especially because the doctors won't tell you that you're ever going to get over it. They won't promise to fix it. Some articles I've read say that if your hands hurt when you aren't doing an activity, then you've got it for life.' She paused. 'I choose not to believe that.'"

In a sidebar, the following tips to reduce the risk of RSI are attributed to a fact-sheet published by the Australian Journalists' Association and a handout distributed by the Australian Council of Trade Unions:

- Adjust the work station so you can assume a comfortable keying

position.

- Try to use a soft touch when keying and avoid over-stretching the fingers.

- Avoid resting your wrists on the keyboard or edge of the desk when typing.

- Don't bend your hands up at the wrists.

- Try to take frequent, short rest breaks, and every half hour or so, do some stretching.

- Don't use painkilling drugs in order to keep working.

- Immediately report symptoms of RSI (persistent pain, tenderness, tingling, or numbness) and seek medical advice.

Safety Officers and "Oversight"

<pyramid!utzoo!henry@hplabs.HP.COM>
Mon, 12 Jan 87 19:38:11 pst

In the February Analog (one of the science-fiction magazines), there is an interesting and partially relevant non-fiction article by Harry Stine. The relevant part is his discussion of certain shuttle safety issues. He was one of the people saying all along that NASA had problems, and in particular he wrote (under his penname "Lee Correy") the SF novel "Shuttle Down", which exposed how utterly unprepared NASA was for an emergency landing by a Vandenberg-launched shuttle. (The only viable landing spot is Easter Island, where landing would have been difficult and dangerous and recovery of the orbiter would have been a monumental problem, since no thought had been given to the issue.) He notes:

"There's talk of a 'safety oversight committee' to review each space shuttle mission before it's launched. But isn't that exactly what NASA had when the Challenger blew up?

"Safety committees don't work in the crunch. One person finally has to decide go-no-go and accept the responsibility which cannot and must not be spread among a committee, where no single person is accountable if something goes wrong..."

He goes on to cite his credentials, including spending some years as Range Safety Officer at White Sands, and being chairman of the group that wrote the standard DoD range-safety rules for rocket ranges.

"There have been some gut-wrenching occurrences. One night I told a well known and politically powerful upper-air scientist [that winds were too high and] the unguided Aerobee would impact off the range. Therefore, I told him he should cancel ... He said he was Project Scientist, he needed the data, the delay would result in a budget over-run, and

therefore he was going to launch. I replied that I would push the destruct button the instant the rocket cleared the launch tower. He launched. I pushed the button. The commanding officer called me into his office the next morning and asked me what happened; I told him. Nothing more was said because the Word of the Safety Officer is as the Word of God. There is no tribunal that can over-rule or second-guess a Safety Officer. There can be no retribution against the Safety Officer. He calls the shots. If he calls too many unsafe ones, the range commander ... transfers him to some other position.

"That decades-old policy works very well. People can be easily trained to use it and be unafraid of invoking it when the need arises. ...

"A safety oversight committee cannot prevent another space shuttle accident. It can either delay the program so badly that it won't make any difference in the long run, or it will mean that nothing gets launched. ... If the automotive industry had a government safety oversight committee riding herd on it, we'd all be walking."

The rest of the article discusses other issues, like how to get the space program in general moving again. One other point he does raise is that NASA tends to be asked for its opinion on the viability and reliability of private launch-vehicle schemes, and as you would expect, its assessments of potential competitors tend to be rather negative...

Henry Spencer @ U of Toronto Zoology
{allegra,ihnp4,decvax,pyramid}!utzoo!henry

Search RISKS using swish-e

THE RISKS DIGEST

Forum on Risks to the Public in Computers and Related Systems

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

Volume 4: Issue 41

Monday, 22 January 1987

Contents

Audi 5000 recall

Dave Platt <dplatt@teknowledge-vaxc.ARPA>
Fri, 16 Jan 87 10:09:47 PST

Audi has announced a total recall of all pre-'87 Audi 5000s equipped with automatic transmissions. The recall is an extension of the earlier, voluntary callback of these cars to equip them with the shift-lock device, and to inspect and if necessary correct the idle valve. Audi is not, at this time, replacing any microprocessor components, nor have they admitted or agreed that any such replacement is necessary.

[The National Highway Traffic Safety Administration has been informed of "5 deaths and 271 injuries related to the problem." PGN]

Air Traffic Control Safety -- 1986

Peter G. Neumann <Neumann@CSL.SRI.COM>
Mon 19 Jan 87 20:06:26-PST

SF Chron 15 Jan 87 via Cox News Service:

Reports of near collisions involving commercial aircraft jumped 37.6%

nationwide in 1986... 329 near collisions involving at least one commercial aircraft... (239 in 1985) 49 of the 1986 accidents were clasified "critical", meaning that chance rather than pilot action prevented a collision... FAA officials dismiss the notion that the air traffic control system is not back up to speed. Agency officials attribute the increase in part to an improved reporting system, heightened public awareness about air safety, and increased air traffic.

SF Chron 16 Jan 87, p 25 (UPI):

Air traffic controllers at Southern California's primary radar center destroyed evidence, falsified reports and lied to investigators to conceal errors that placed airplanes on collision courses... [quoting article from th Orange County Register]

"On February 16, an 18-passenger Skywest Airlines commuter jet and a six-passenger private plane were within 3.8 miles of each other and on a collision course when an air traffic controller reportedly turned off the computer that was tracking them." ...

"On February 13, a conflict alert signal went off three times, warning a controller that a 105-passenger DC-9 and a 12-passenger private jet were within 2.5 miles of each other and on a collision course. ... the controller turned off the alert each time to try to conceal his error."

UK EFT Risks

Brian Randell <brian%kelpie.newcastle.ac.uk@Cs.Ucl.AC.UK>
Mon, 19 Jan 87 13:00:21 gmt

EXTENT OF UK EFT RISKS

The Jan 15 issue of Computer News carried an account of a talk by Detective Inspector John Austen of the Computer Crime Unit at New Scotland Yard which contained statistics and comments about the use of EFT in the UK, and of the possible risks due to criminal action. It is contained in a lengthy article describing a BCS Security Committee Seminar for the National Computer Users' Forum, held recently in London. I found the following comments, especially the statistics quoted, particularly interesting/alarming, so thought them worth reporting to RISKS:

"EFT now represents 83% of the value of all things paid for - money transferred - in Britain. Money, as an invisible export is a major and vital part of our GNP. Foreign exchange markets in London transfer $200bn daily using EFT via satellite. The transactions take a very short time, and once complete there is no calling them back. A lot of people are aware of this. And many, both here and abroad, are prepared to steal from EFT systems. The rewards are tremendous."

"Companies, and even the economies of smaller countries, could be crippled by a sustained hit on EFT systems. Terrorists, such as the Middle East

factions, the IRA and the Red Army Faction are particularly aware of this - and they need money. The Red aRmy Faction has already, unsuccessfully, made moves to intercept EFT in Germany. They and others will try again."

Brian Randell - Computing Laboratory, University of Newcastle upon Tyne

ARPA : brian%cheviot.newcastle.ac.uk@cs.ucl.ac.uk
UUCP : <UK>!ukc!cheviot!brian
JANET : brian@uk.ac.newcastle.cheviot

Another Bank Card Horror Story

Dave Wortman <dw%csri.toronto.edu@RELAY.CS.NET>
Mon, 19 Jan 87 10:51:12 est

The automatic teller machines (ATMs) supported by our local bank are fairly typical. Each customer has a magic card that references a checking account, a savings account, a credit card and perhaps some other accounts. These are called "checking", "savings", "other#1", etc. The ATM system never discloses the real account number. I recently had a very disconcerting run in with this system. My bank card and accounts have been in existence for several years. Recently I went to my local bank and opened a new account.

Unbeknownst to me, the act of opening a new account changed the designation of accounts on my bank card. What had been my primary checking account was bumped to other#3 and my new account became my primary checking account. Apparently the bank card uses indirect references since these changes happened some night without the bank getting their hands on my card. I do not know if the problem was a human error in the setting up of my new account or a programming error in the ATM system software.

I was lucky, the new account I opened happened to be in a foreign currency and so the ATMs started rejecting all transactions against my "checking" account. I discovered the explanation given above only after a couple of frustrating weeks and a couple visits to my bank.

Things could have been a lot worse! If the new account had not been rejected immediately by the ATM then I might not have discovered the problem until the next round of bank statements a month or so hence. In the meantime my accounts could have become hopelessly fouled up.

Independent of whether my problem was caused by a processing error or by a software error, I think my experience demonstrates several inadequacies in the design of the ATM "system".

1. the carefully negotiated interface between the user and the bank should NEVER change without the knowledge of both parties. Normal procedure is for it to change only upon written request by the user.

2. There should be a better mechanism for the user to verify that the interface defined by the bank card corresponds exactly to the user's expectations.

3. There should be more immediate feedback in the system in the case of errors or changes. Because of the foreign currency problem described above, I happened to get a fairly immediate indication that something was wrong. In the worst case, I might have not received any indication that something was wrong until the first bank statements for the new account arrived (typically 1.5 MONTHS).

Stock Market behavior

Rob Horn <wanginst!infinet!rhorn@harvard.HARVARD.EDU>
Thu, 15 Jan 87 22:13:57 est

The impact of computer trading on the stock market, and in particular the ``triple witching hour,'' has not gone unattended by the stock market directors and regulators. Their response has shown considerably more insight into market behavior than might be expected. They have not considered computers to be the problem.

The problem of the ``triple witching hour'' is that during a few hours on the third friday of each third month (typically from 3-4PM) there is an immense burst of market activity as major participants rearrange their computer selected portfolios. (This particular time is triggered by the expiration time of a key financial component in these ``computer based'' trades.) Before these trading programs, hearing that someone needs to sell 100,000 shares of IBM quick, like in the next 5 minutes, meant that there was a major problem at IBM. Many people still react in panic when they hear such news. These habits and expectations where being greatly shocked by massive shifts like this which merely reflected trivial adjustments between stock prices and interest rates.

For the previous two witching hours, and for the forseeable future, market makers are now required to publish their required major stock trades several hours in advance on these Fridays. This gives all the other participants time to evaluate the trades and determine what they mean. It also seems to be working. Both Friday's had trading volumes just as huge as other such Fridays, but did not suffer from the sudden pricing shocks. Prices were quite well behaved with no unusual changes.

Based on prior behavior the odds that two in a row would be this orderly is between 10-20%. March really tell whether this added information flow is really all that is necessary for the stock market participants to properly interpret the meanings of these massive stock trades. It does look promising.

Rob Horn
UUCP: ...{decvax, seismo!harvard}!wanginst!infinet!rhorn
Snail: Infinet, 40 High St., North Andover, MA

Report problems with the web pages to the maintainer

Search RISKS using swish-e

THE RISKS DIGEST

Forum on Risks to the Public in Computers and Related Systems

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

Volume 4: Issue 42

Friday, 23 January 1987

Contents

A scary tale--Sperry avionics module testing bites the dust?

Nancy Leveson <nancy@ICSD.UCI.EDU>
21 Jan 87 12:53:51 PST (Wed)

I just spoke to a man at the FAA who is involved with aircraft certification. He told me that Sperry Avionics, who are building the computerized automatic pilot among other things for a future new aircraft, is trying to convince them to eliminate module testing for the software. According to this man, Sperry argues that programmers find module testing too boring and won't stay around to do it. Instead of module testing, Sperry wants to use n-version programming and perform only functional system test. As long as the results from the two channels match, they will assume they are correct.

I am not concerned that they are using n-version programming, but that

they are arguing that the use of it justifies eliminating something that is considered reasonable software engineering practice. The FAA has agreed to allow them to try this. According to my FAA source, the FAA is not thoroughly comfortable with this, but the autopilot is only flight-crucial on this aircraft during about 45 seconds of the landing. Also, their tests have found that pilots can successfully recover from an autopilot failure during this period (by performing a go-around) about 80% of the time.

I am going to talk further about this with some people at the FAA who are involved with certification. If anyone else shares my concern (or would like to allay my fears), I would appreciate hearing your opinions and arguments. I will convey them to the FAA unless you state that they should remain confidential.

Nancy Leveson (nancy@ics.uci.edu)

(P.S. Anybody want to join me in writing Congress about saving Amtrak?)

Computer gotcha

Dave Emery <emery@mitre-bedford.ARPA>
Tue, 20 Jan 87 15:12:04 est

Here's a computer gotcha for you...

Like many other people, I was trying to close on a new house before the end of the year, for tax reasons. We had our down payment wired from our bank in New Jersey to our bank in New Hampshire, supposedly a fail-safe transaction. Unfortunately, the Bank of New England, which was (one of) the middleman in the wire transfer failed. Apparently, their system was overloaded, and crashed.

My mother is a teller in a bank in Pittsburgh. She says that, at least at her bank, system crashes are a way of life. Fortunately, she says, they rarely lose any money.

Dave Emery, MITRE Corp, Bedford MA

P.S. Bank of New England recovered later that day, and we got our money after we signed the papers. The legal transaction was recorded the following day.

Re: Another Bank Card Horror Story

<Frankston@MIT-MULTICS.ARPA>
Tue, 20 Jan 87 23:42 EST

The issue of ATM accountability reminds me of a problem I am having untangling my Mastercard transactions here. In general, the reports generated on the statements fail to provide the minimal information necessary for untangling messes. Information like which card was actually used is entirely missing. Only American Express seems to understand that each instance of a card should be tagged. This is especially annoying when the bank doesn't seem to mind that a stolen card is used for 8 months to buy tickets on the Eastern Shuttle. Credit transactions don't give a hint as to

what transactions they are being counted against.

While some of this just reflects ineptness and neglect in the bank's DP department, it also is indicative of what is going to become a real issue as we attempt to connect our personal computers with existing services. (or even banks connect to each other). Electronic banking services in general do an inadequate job of export/import of data. Such concepts as unique ID's for tagging and tracking transactions don't really exist. In the previous mastercard card example, the transaction id is just some characters associated with the transactions and are likely to not be unique. It seems as if my home processing of this information is more sophisticated than the bank's!

It reminds me of my attempt to setup an equipment tagging system. I decided to order two sets of tags -- red for permanent stickers and black for removeables so that we can tag loaner equipment. The office manager followed through on this but both sets were numbered from 1 to 1000. It was difficult to explain why this was a problem since it was obvious which was red and which was black.

The problems are manifestations of the issue of fundamental information processing literacy. While some of us working with computers have learned techniques to deal with aspects of this, the knowledge is not well distributed through society, nor even the DP profession. But the use of computers is becoming pervasive.

This conflict is at the heart of a large class of computer-based risks. In the short term, the best we can do is point out the issues. Pointing out solutions is harder -- especially when they are obvious to us. The real question is how we can convey this understanding to the society at large.

Are there any references that exist to try to explain the concepts of dealing with complicated systems and their interactions? Maybe even gather a list of such obvious things as checksums (and limitations on simple checksums), unique ids (and the low cost of using a lot of integers), redundancy (and its low cost/benefit) etc.

On the other hand, maybe these difficulties are really blessings since an efficient EFT system, for example, might be a serious threat to privacy so that these annoyances and even risks are worth it till we understand how to deal with the system once it works smoothly.

RISKS 4.41, Stock Market behavior

Howard Israel <HIsrael@DOCKMASTER.ARPA>
Tue, 20 Jan 87 16:17 EST

>For the previous two witching hours, and for the forseeable future, market
>makers are now required to publish their required major stock trades several
>hours in advance on these Fridays.

Minor correction. According to the Washington Post business section that

described this new SEC strategy of disclosure, it is not "required", but recommended. All major brokerages complied except one (I believe it was Drexel Burnham Lambert Inc.), which caused a minor fervor as traders acted on "incomplete information", thus giving Drexel a slight advantage. Drexel was criticized for not disclosing their intended trades but countered that it did not violate any SEC "rules" and thus acted properly.

The intended affect of the disclosure is to give traders advance notice, in effect, reducing the "shock" factor as well as allowing the "market makers" to adjust their inventories of stocks to prepare for the expected orders.

Note: that a trade can be put in by a trader to be executed "at the market closing price" for a given stock. Regardless of what the price is, the trade will be executed. The deluge of orders on the "triple witching hour" at the "market closing price" often caused the ticker to be delayed up to a half hour at the closing.

Stock Market behavior

<kremen@aerospace.ARPA>
Wed, 21 Jan 87 13:48:33 -0800

>The problem of the ``triple witching hour'' is that during a few hours on
>the third friday of each third month (typically from 3-4PM) there is an
>immense burst of market activity as major participants rearrange their
>computer selected portfolios. (This particular time is triggered by the
>expiration time of a key financial component in these ``computer based''
>trades.)

Not really true, most of the problem occurs in the last 10 minutes of trading when the "unwinding" of stock index futures, options on those futures, and the underlying equities occur. Usually the brunt of the unwinding occurs in Chicago, where the futures are traded. We only see a portion of this when one looks at the volume on the New York Stock Exchange. Also, not all unwinding occurs on "expiration day". If conditions are favorable, stock positions can be unwound earlier.

>Before these trading programs, hearing that someone needs to sell 100,000
>shares of IBM quick, like in the next 5 minutes, meant that there was a
>major problem at IBM. Many people still react in panic when they hear
>such news.

NO ONE panics. Since 1982, when stock market indexes (such as the Major Market Index or the S&P 100) started to be traded, the "triple witching hours" have occurred. Only within the past two years have the underlying markets been liquid enought to make it really worthwhile. Anyway institutions frequently sell (or buy) 100,000 shares of IBM for normal trading purposes. [...]

For more information see the December 29, 1986 issue of Insight magazine.

Engineering models applied to systems

Alan Wexelblat <wex@mcc.com>
Tue, 20 Jan 87 10:49:53 CST

In Burnham's _The Rise of the Computer State_, MIT Professor Jeffrey A. Meldman is quoted as follows:

> "In engineering, there is a principle which holds that it is frequently best to have a loosely-coupled system. The problem with tightly coupled systems is that should a bad vibration start at one end of the machine, it will readiate and may cause difficulties in all parts of the system. Loose coupling is frequently essential to keep a large structure from falling down. I think this principle of mechanical engineering may be applicable to the way we use computers in the United States."

The context of the quote is a chapter on the aggregations of power that can accrue in large, centralized computer systems and the risks (and temptations) of abuse of this power.

RISKS readers have previously dismissed other engineering models as inapplicable to software systems. Comments on this one?

Alan Wexelblat
ARPA: WEX@MCC.ARPA or WEX@MCC.COM
UUCP: {seismo, harvard, gatech, pyramid, &c.}!ut-sally!im4u!milano!wex

---

Re: British EFT note

Alan Wexelblat <wex@mcc.com>
Tue, 20 Jan 87 10:54:42 CST

It is worth reminding RISKS readers that a British "billion" is a million millions (1,000,000,000,000) rather than the American thousand millions (1,000,000,000). --Alan Wexelblat

> [This was also noted by Howard Israel. By the way, I observe that the BBC radio broadcasts on PBS now routinely use "thousand million" and "million million"... PGN]

Train Wreck Inquiry (Risks 2.9)

<Matthew_Kruk%UBC.MAILNET@MIT-MULTICS.ARPA>
Fri, 23 Jan 87 08:46:12 PST

Just caught bits and pieces on the morning radio news about this item mentioned in Risks 2.9:

An inquiry into the collision between a VIA passenger train and a Canadian National freight train near Hinton, Alberta last year, has put the blame on human error. The freight crew were said to have ignored various safety

procedures. Also, Canadian National was accused of ignoring too many minor safety infractions and for letting crews work without sufficient rest periods between shifts.

Computer error was not mentioned as a contributing factor.

Cost-benefit analyses and automobile recalls (RISKS DIGEST 4.39)

John Chambers <jc@cdx39.UUCP>
23 Jan 87 19:06:07 GMT

> Moreover, even if the [cost-benefit] analyses were performed
> correctly, the results could be socially unacceptable. [...] In the
> case of automobile recalls, where the sample size is much larger, the
> manufacturers may already be trading off the cost of a recall against
> the expected cost of resulting lawsuits, although I hope not.

Sure they are. Have you ever heard of "liability insurance"?

There is also the general observation that, the way most forms of cost-benefit analysis work, ignoring (i.e., failing to assign an explicit value to) some factor is mathematically equivalent to assigning it a cost of zero. In other words, a cost-benefit analysis can't generally distiguish an unknown cost from a zero cost. Similarly for benefits.

> The "value of a human life" is not a constant. The life of a volunteer or
> professional, expended in the line of duty, has always been considered less
> costly than the life of innocents.

Huh? Most military organizations that I've heard of consider the cost of training a soldier to be significant; the value of innocents (i.e., civilians) is generally ignored, and thus considered to be zero. This was painfully obvious during the Vietnamese war, for instance.

> As for the dangers of incorrectly estimating risks, I think that the
> real danger is in not estimating risks.

If you listen to public discussions of risky situations, it soon becomes quite clear that few people are able to distinguish "We know of no risks" from "We know there are no risks".

...

> One can only imagine the reaction of the program authors when they
> discovered what one last small change to the program's scoring function
> was necessary to make it match the panel's results. It raises
> interesting questions of whistle-blowing.

Even if the programmers looked at the regression function, it's not clear that they would have even seen a racial component. For a nice example of how things can go wrong, consider that you can

do a rather good job of sex discrimination while totally ignoring
sex; you just use the person's height instead. There have been
published studies that imply that this is widespread practice;
it's been known for some years that [in the USA] a person's height
is a better predictor of their income than their sex, and if height
is included, knowing their sex adds no further information. It's
likely that in the UK there are several attributes that are strongly
correlated with race, so you need not necessarily use race at all.

John M Chambers Phone: 617/364-2000x7304
Email: ...{adelie,bu-cs,harvax,inmet,mcsbos,mit-eddie,mot[bos]}!cdx39!{jc,news,root,usenet,uucp}
Codex Corporation; Mailstop C1-30; 20 Cabot Blvd; Mansfield MA 02048-1193

Search RISKS using swish-e

THE RISKS DIGEST

Forum on Risks to the Public in Computers and Related Systems

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

Volume 4: Issue 43

Monday, 26 January 1987

Contents

"Cable `Hackers' Claim Scrambler is History"; other breaches

Peter G. Neumann <Neumann@CSL.SRI.COM>
Mon 26 Jan 87 21:05:14-PST

SF Chron 26 Jan 87, page 3 (from UPI):

A year-old "unbreakable" scrambler that has kept satellite dish owners from receiving pay television channels free has been broken...

The article describes the "Three Musketeers" chip, which you can use to replace a chip in the $395 decoder if you have any legitimate pay channel. It then goes on to quote Captain Midnight, who claims that an even more devastating breach has been discovered that does not even require the "Three Musketeers" chip! He recommends you not waste your money on the hot chip.

By the way, recently SECURITY@RUTGERS has had quite a few items of interest to RISKS readers. Here are two:

Given an Ethernet board, you can read ALL of the network traffic by

flipping a single bit.

A Sun System security breach was described, compromised via unpassworded special accounts.

Some of the experiments with Gould's allegedly secure UNIX.

Re: VideoCypher II

Michael Grant <mgrant@mimsy.umd.edu>
Sat, 24 Jan 87 12:24:06 EST

>David Platt notes:
>If, for example, the box had been provided with a cover-removal switch that
>would signal the micro to erase it's subscriber number...

Always best to eliminate the problem by redesigning that part in the next generation of the cypher so that such important numbers as that never leave the internals of chips. At that point, it becomes much more of a pain to probe than it may be worth, but...not entirly imposible.

Douglas Humphrey <deh@eneevax.umd.edu>
Sun, 25 Jan 87 14:42:09 EST

security@rutgers.rutgers.edu
Subject: Re: DES cracked?

>Way #3: someone's actually found a way of identifying the key of a DES
>transmission, with (or possibly without) the unscrambled "plaintext"
>audio as a starting point.

Note that they can easily have the plaintext, since the best way to start experimenting on breaking something is to have two devices there, one subscribed and authorized, and the other not. That way you have (subject to trivial timing differences which can be ironed out) two streams of data to play with, and you really are just trying to make one look like the other.

On another note, does anyone know of any good spectrum analysis software available for cheap to work with reasonable priced A/D converters ? There are a number of companies that sell the hardware required to eat signals, but most of the software that I have seen for actualy analysing the data is pretty weak. Maybe I'm just not in touch with the right companies...

Doug

Re: Billions

Brian Randell <brian%kelpie.newcastle.ac.uk@Cs.Ucl.AC.UK>
Mon, 26 Jan 87 18:37:17 gmt

Oops! Sorry - I am usually more careful about transatlantic differences in the meaning of "billion", though (regretfully) there is a growing tendency for at least the popular newspapers in the UK to conform to US usage re "billion", presumably because a "billion" is shorter and sounds more impressive than "a thousandmillion" and few people know that the proper English (or, if you insist, British) term for this is "milliard" - a term which does not seem to exist in American.

In fact my Webster's Dictionary (I smuggled one into the UK with me when I left IBM) tells me that above one million, all the names differ across the Atlantic, even "septillion", "quattuordecillion", "novemdecillion", etc.

I wonder whether any actual (computer-based) risks have arisen to the public from this confusion over billion - to match those that surely must have arisen over imperial vs metric scales, celsius vs fahrenheit, etc. For example, Edsger Dijkstra told me once of a remote manipulator built for the Anglo-Dutch firm Shell Oil which was usable only by a giant because it was built in metres instead of feet. And I recall, from my early days with the Atomic Power Division of English Electric, that our nuclear reactor codes had to deal with reactor designs in which the coolant entered a heat-exchanger (from something designed by physicists) in degrees centigrade (as it then was) and left (this domain of engineers) in degrees fahrenheit.

Cheers, Brian

[One such case was the Discovery laser experiment, which aimed upward to a point 10,023 MILES above sea level instead of downward to a point 10,023 FEET above sea level (a mountain top). Another was the $.5M transaction that became $500M because of nonagreement on units. Both (coincidentally) are described in Software Engineering Notes vol 10 no 3, which appeared just before the on-line RISKS Forum began. PGN]

GM On-Board Computers [lightly edited]

"Wes Williams" <GZT.EWW%OZ.AI.MIT.EDU@XX.LCS.MIT.EDU>
Sat 24 Jan 87 11:20:49-EST

As I have spent some time in the automotive repair field, I have come across an anomaly when General Motors' main computer system repairs are performed. I share it with you here.

In two years after 1980 (the year when GM installed an on-board computer on the vast majority of its models) the repair facilities had a tendency to replace the complete computer assembly rather than troubleshoot the problem extensively. This was the transition period. Repair people were unfamiliar with the approriate procedures and also had a tendency to replace (Well I ain't ever done one of these before, boss!) rather than understand and repair an associated problem.

During these two years, I replaced only two computers. One was from a car involved in an electrical fire, the other was in a car that had collision damage on the right side, close to the computer, and the computer was damaged (visibly).

In 1985 I was troubleshooting a 1981 Cadillac that had the infamous 8-6-4 engine with a power-on stutter. I found a broken (cracked) distributor cap and saw High voltage (30-60,000 volts) shooting from the cap to the lead that was coming from the computer. This was the electronic timing advance control circuit. I replaced the bad cap, retested the car, and found that the problem was better but had not disappeared. All other associated tests were performed and no other problems were found except that the diagnostics generated by the on-board computer were all out of whack. On this model Caddy, if you press the climate control buttons you will get a diagnostic check run off by the cpu. The readout comes out as two-digit numbers on the temperature control. These numbers were never the same, and some were not within the diagnostic capability of the cpu.

I was now in the position of the other fellows and said, "Well, gotta replace the cpu." A logical conclusion, knowing that the readout was not right, as well as seeing high voltages heading for the cpu.

I pulled the cpu, headed for GM parts and was shocked to learn that I could not purchase a complete unit (proms included), I had to remove the old proms and install them in the "rebuilt" computer. Seemed a little dumb when the cpu was subjected to high voltages, to keep the old proms.

After the change of cpu's and installation of old proms, there was no change in the operation of the engine. I quit and gave the car to Cadillac to repair. They spent untold hours on it, communicated with the Caddy hot line, had service reps around from the factory and made a large number of updates to a variety of systems as well as unnecessary other changes. Total bill? = $0.00. Even they couldn't fix it. It is running better, the stutter is still there, the car is on the road and getting slightly lower than average mileage. (sigh)

Summary: To GM --> Why can't one replace the proms to the CPU. Are they burned in with detailed specific instructions according to each cars engine performance?

To the public--> when a GM computer is replaced, the "core charge" or trade-in on the malfunctioning cpu is close to $300.00, so that drops the price of the cpu from $500.00 to $200.00. Watch your bills here!! (These figures are + or - $50.00 for the component only, not the labor.)

To the technical types. --> It would seem feasible to design a program and attaching hardware to diagnose (at least one type (say GM)) of an on-board computer with a P.C. I know that Caddy spent at least 40 hours on this problem. At the labor rate of $38.00 per hour and knowing that there are other similar occurrences, there has to be some money to be made in the purchase of such a system as well as the sale.

Quote 1: "Not knowing the answer is only being uneducated."

Quote 2: "Not knowing where to look for the answer is being 'uninformed'."

Quote 3: "When the product is a common one, and none know where to look for the answer, nor know it, this is truly ignorance."

Active control of skyscrapers

"Peter G. Capek" <CAPEK@ibm.com>
26 January 1987, 20:37:17 EST

Catching up on my reading, I noticed the recent discussion in RISKS about active control of skyscrapers. If this is still of interest, I offer the following excerpts from an article I happened across some years ago and clipped. It appeared in Engineering News Record, August 18, 1977.

TUNE MASS DAMPERS STEADY SWAY OF SKYSCRAPERS IN WIND

A 50-year-old idea of using the inertia of a heavy floating mass to tame the sway of a tall building is now getting its first real tryout in New York City and Boston skyscrapers. Citicorp Center in New York and Boston's Hancock Tower are newly fitted out with so-called tuned mass dampers, the first in tall buildings in the U.S., according to the designers of the systems, structural consultant LeMessurier Associates/SCI, Cambridge, Mass, and MTS Systems Corp., the manufacturer, Minneapolis.

A tuned mass damper (TMD) consists of a heavy weight installed near a building's top in such a way that it tends to remain still while the building moves beneath it and in away that it can transmit this inertia to the building's frame, thereby reducing the building's motion.

The mass itself need weigh only 0.25% to 0.75% of the building's total weight. When activated, it becomes free-floating (or "levitates" as its designers like to say) by rising on a nearly frictionless film of oil. Piston-like connectors, which are pneumatic springs in which pistons react against compressed nitrogen, are attached both to the mass and the building frame so that as the building sways away from the mass, the springs pull the building pack to the center.

"Tuned" simply means the mass can be caused to move in a natural period equal to the building's natural period so that it will be more effective in counteracting the building's motion. During a heavy wind storm, the mass might appear to move in relation to the building some 2 to 4 ft. ...

A TMD is a device to minimize the discomfort experienced by occupants when a building is swaying. As such, it can be used in place of adding structural steel to stiffen a building or adding concerete to weigh it down, which designers say is a much more costly way of reducing uncomfortable levels of motion. To the engineers who designed it, the TMD is a positive approach to relieving wind-induced building motion because it counteracts motion rather than first receiving it and then deadening it, which is the inefficient and more costly result of substantially increasing mass or stiffness. ...

A TMD's advantage becomes academic in a power failure. It needs electricity to work and if that's lost in a heavey wind storm, when the TMD would be most needed, it won't work. ...

The TMD designed for Citicorp's slender 914-foot tower in midtown Manhattan has a mass block of concrete 30 x 30 x 10 feet, with cutouts for attachments, that weighs 400 tons. It has two spring-damping mechanisms, one to counteract north-south motion and one for east-west motion. It also has an antiyaw device to prevent the mass block from twisting, a failsafe device consisting of shock absorbers and sunbbers to resist excessive or eccentric motion, and a control system that collects data on the building's motion and controls the response of the mass. It is located in a speciall designed space in the building's 59th floor, which is supported by trusses below. It is designed to activate at an acceleration of 3 milli-g's, which could be caused by about a 40-mph wind, and it is designed to prevent the building from deflecting more than 12 to 13 inches.

LeMessurier estimates Citicorp's TMD, which cost about $1.5 million, saved overall a possible $3.5 to $4 million that would have been spent to add some 28,000 tons of structural steel to stiffen the frame and floor concrete to add weight.

The TMD for the John Hancock Mutual Life Insurance Co.'s glass-clad landmark in Boston is somewhat different. First of all ... it was added as an afterthought when architect I.M. Pei & Partners realized that the building had insufficient wind bracing to prevent occupant discomfort. Secondly, Hancock Tower is rectangular in plan and is a frame building, unlike Citicorp's essentially bearing wall structure. For Hancock, then, LeMessurier placed two TMD's, one at either end of the 58th floor. Because of the building's shape and location, it must counteract mainly east-west winds and a twisting force. The dampers, then, move only in an east-west direction and can be induced to work together or in opposition to stablize the building. They are located 220 feet apart, and when moving in opposition act in effect as a 220-ft lever arm to resist twisting. A Hancock building official wouldn't reveal what it cost to add the dampers, which designers say could reduce the building's swaying motion a full 40 to 50% under what it had originally been designed for. ...

Peter G. Capek, IBM Research -- Yorktown Heights, New York

Search RISKS using swish-e

Report problems with the web pages to the maintainer

Search RISKS using swish-e

THE RISKS DIGEST

Forum on Risks to the Public in Computers and Related Systems

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

Volume 4: Issue 44

Thursday, 29 January 1987

Contents

Air Traffic Control -- More Mid-Air Collisions and Prevention

Peter G. Neumann <Neumann@CSL.SRI.COM>
Thu 29 Jan 87 20:12:19-PST

There were several collisions recently that are worthy of note here.

A twin-engine 18-seat Metroliner and a single-engine private plane collided near Salt Lake City on 15 January 1987. All 10 aboard killed. The small plane had no altitude transponder.

An Army twin-enginer turboprop collided with a twin-engine business plane near Independence, MO. All 6 people killed. 19 January 1987. Both planes had altitude transponders, but controllers said they did not see the altitude data on their screens.

A six-seat regional airliner and a single-engine private plane grazed

each other near Westerly, RI. No one hurt. 19 January 1987.

The FAA is contemplating extending its forthcoming Mode-C regulations to include commuter planes as well as mainliners. [Source: SFChron 25 Jan 87]

Time warp for Honeywell CP-6 sites

<PHiggins@UCIVMSA.BITNET>
Thu, 29-JAN-1987 10:30 PST

All Honeywell CP-6 sites running version C01 of CP-6 suddenly entered a time warp Wednesday morning. The Front End Processor (FEP) suddenly thought it was December of 1968, but the host still knew the correct time and date. It turns out that the sign bit of the word containing the time finally got set. Unfortunately, that word appears to have been declared as a signed number rather than an unsigned one. (How you could ever have a negative time is beyond me.) Since the base time for CP-6 is January 1, 1978, we suddenly scooted back in time to 1968. The problem was first reported by a CP-6 site in Germany at 5:23am Pacific Standard Time.

What impact did this have on CP-6 users? Those using programs running solely on the host weren't affected, though the login message gave the wrong time and date. Those using the Transaction Processing (TP) features of the FEP, however, discovered that incorrect dates were entered into their databases on the host. CP-6 sites are now manually correcting the bad data.

The problem was fixed by early Wednesday afternoon and a patch was made available to Honeywell's customers.

By the way, one CP-6 site determined that the time stamp will overflow at 15:26:07.35 on October 11, 1999. Mark that down on your calendars!

Here's the message Honeywell sent to its customers. (A STAR is a problem report.)

> Sent: 01/28/87 06:39 Rcvd: 01/28/87 06:53 Number: 68
> To: CUSTOMERS,CP-6 FOLKS From: (deleted)
> Subject: FEP timestamp problem
>
> Yes, good morning y'all. The CP-6 interpretation of the level-6 timestamp seems to have started to pickup a sign bit today, so every site in the world, regardless of patch revision or system revision is happy, happy, happy. Star 32173 has been generated to track this problem at severity one. If you want to be on the list of people to be notified as soon as a fix is available, please build a note on that star. Sorry 'bout that.

GM On-Board Computers

Martin Harriman <"SRUCAD::MARTIN%sc.intel.com"@RELAY.CS.NET>

Wed, 28 Jan 87 15:24 PDT

The reason that the ROMs on the GM Engine Control Module do not come with the replacement unit is that they are specific to the automobile--they vary, depending on the particular automobile model, engine, and transmission. This is no different from a number of other components (distributor innards in older cars, for instance). The ROMs are available (on special order) as replacement parts; you need to know the exact configuration of your GM car to order them (that is, the VIN, the engine code, and the transmission code--I don't think you need the complete set of option order codes, though these are usually available on a sticker buried in the trunk). The ECMs are generic (there have only been a few major revisions of the basic module), and the ROMs are (extremely) specific--so it is not possible to stock the complete set of ROMs, nor to stock ECMs with ROMs installed.

There are several specialized tools available for ECM based diagnostics. For field use, several companies make special tools which plug in to a connector under the dash, and communicate with the ECM to monitor engine parameters and diagnose faults. This is an amazingly powerful tool for diagnosing engine problems; you can, for instance, see if the engine tends to run rich or lean in one particular regime by reading out the current "block learn mode" matrix from the ECM (this is a set of fudge factors the ECM keeps so it can guess at the correct fuel delivery for your particular car and engine). All GM dealers should have such tools, and (presumably) know how to use them.

Incidentally, you can read out some of the ECM diagnostics with nothing fancier than a bent paperclip; the GM shop manuals give all the details. This is most useful in a case where the ECM has already found a problem, and illuminated the "Service Engine Soon" light (the ECM checks all its sensor values for "reasonableness"; if things don't seem right, it complains).

Loose coupling

<decvax!wanginst!wang!ephraim@ucbvax.Berkeley.EDU>
Wed, 28 Jan 87 20:25:34 est

In Risks 4.42, Alan Wexelblat asks about the applicability of the principle of "loose coupling" to computer systems. I think the principle is a valuable one. Herewith, a brief study in contrast.

My present employer, Wang Labs, makes a variety of computer systems. The Wang VS series are conventional minicomputers. That is, they have a cpu which runs user tasks, with a conventional OS. The Wang OIS is a loosely-coupled system in which a central file server (the OIS "master") supports a collection of workstations and peripheral devices. The VS, which is probably no better or worse than most computers of its class, suffers occasionally from task crashes and OS crashes. Installation of new peripherals or major new software generally requires an IPL or two. On the OIS, all user code runs in the workstation. If your workstation (or other peripheral) crashes, the most that's required is to cycle power on the

device. The master sees the power-up, and reloads you. *All* OIS software except the master code can be re-installed without an IPL. Peripherals can be installed simply by plugging them in.

In a development environment, VS's are sometimes reloaded hourly in order to change software, change configuration, or recover from crashes. (Released software, of course, is orders of magnitude more stable.) OIS's? The last time mine was IPLed was to recover from a mechanical disk failure, months ago. Master crashes are practically unheard of.

Generally, I think loose coupling presents an invaluable opportunity for bullet-proofing of components. It becomes possible to validate your input and to recover from external problems, only when "input" and "external" are well-defined terms. Let the lines be drawn.

Disclaimer: These are my own opinions about Wang products. Other Wang employees, salesmen, and customers have their own opinions.

Ephraim Vishniac, decvax!wanginst!wang!ephraim

Units RISKS and also a book to read

"Lindsay F. Marshall" <lindsay%cheviot.newcastle.ac.uk@Cs.Ucl.AC.UK>
Tue, 27 Jan 87 16:29:56 GMT

Another classic case of mistaken magnitude is documented in a variety of books on the CIA. When they were carrying out their infamous LSD experiments they heard that Sandoz had for sale 22lbs of LSD and being so afraid that the Russians would buy, put $250,000 in a case and went shopping. The people at Sandoz looked very puzzled - they had only ever made about the 0.5 oz of the drug. Someone in the CIA Swiss office didn't know the difference between milligrams and kilograms.

I just finished a quite entertaining book featuring a computer crimes investigator of the year 2000. The technical stuff is OK (for a change) and the basic idea behind the plot is quite feasible (and scary!!) from a RISKS point of view. The book is :

Downtime
by Peter Fox
ISBN 0-340-39362-9

Published 1986 by Hodder & SToughton (in the UK at least)
Lindsay

Re: Unit conversion errors

Alan M. Marcum, Consulting <marcum@Sun.COM>
Tue, 27 Jan 87 10:45:25 PST

A unit conversion error (pounds and kilograms, if I recall) was a major

contributing factor in the Air Canada 767 flameout incident a few years ago. The jet ran out of fuel during cruise; the pilot also flew sailplanes, the co-pilot trained near (90 miles away from) the flameout site, and they were able to land safely.

Alan M. Marcum Sun Microsystems, Technical Consulting
marcum@nescorna.Sun.COM Mountain View, California

Units

"Keith F. Lynch" <KFL%MX.LCS.MIT.EDU@MC.LCS.MIT.EDU>
Wed, 28 Jan 87 00:04:03 EST

I think it goes like this:

Power of ten	American name	British name	Metric prefix
3	Thousand	Thousand	Kilo
6	Million	Million	Mega
9	Billion	Milliard	Giga
12	Trillion	Billion	Tera
15	Quadrillion		
18	Quintillion	Trillion	
21	Sextillion		
24	Septillion	Quadrillion	
27	Octillion		
30	Nonillion	Quintillion	

The problem is not that different names are used, but that the same names are used for very different numbers. This is why metric prefixes have caught on. For instance a thousand million electron volts is now called a GEV (for Giga) rather than a BEV (for Billion).

Unfortunately, the metric prefixes don't go very far. In any case, they are hard to remember. And they are no longer always unambiguous, at least in the computer world, where the prefix Mega may mean 1,000,000 or 1,048,576 or even 1,024,000.

The best solution is to use the exponents of ten. Instead of GEV, just say 1E9 EV. This is catching on rapidly, perhaps due to computers, which are more easily programmed to say 1.02E+09 than 1.02 GEV, etc.

You are right, Milliard is not used in the United States. Actually, the highest name I ever hear is trillion. People who speak of quadrillions tend to get funny looks.

[Wait until our national budget gets there in a few years! PGN]

Science meets engineering where I work, too. This results in code where a distance is always stored as millimeters, but is output and read in in mills (thousandths of an inch). Similarly with degrees C and F. Sometimes fully a third of my programming time is taken up with making sure incompatible

units don't mix, and making extra sure whether I multiply or divide by a conversion factor or its inverse, etc.

I discovered a bug in someone else's code where a unit was BTUs per cubic foot per degree F and was later used as calories per cubic centimeter per degree C. I spent a whole day fixing this, before working out the actual conversion factor to put in the constants section - and the conversion factor was exactly 1.

...Keith

DP Ethics: The "Stanley House" Criteria

Pete McVay -- VRO 5-1/D7 --DTN 273-3106 <mcvay%telcom.DEC@decwrl.DEC.COM>
Wednesday, 28 Jan 1987 06:48:37-PST

In 1976, the Canadian government sponsored a meeting in Quebec at the "Stanley House", composed of top data processing experts and philosophers. The meeting specifically addressed the issue of ethical conduct in the computer industry. The list that follows was extracted from an article published that year in SCIENCE Magazine (the official magazine of AAAS). Unfortunately, I do not have the date of the magazine.

I have not heard of any followup on these criteria, either in a discussion on computer risks or ethics, or as any meaningful attempt to implement them. I present them here to RISKS DIGEST for comments by other readers--and perhaps someone has some later information?

Stanley House Criteria for
Humanizing Information Systems

1. Procedures for dealing with users.

   A. The language of a system should be easy to understand.
   B. Transactions with a system should be courteous.
   C. A system should be quick to react.
   D. A system should respond quickly to users (if it is unable to resolve its intended procedure).
   E. A system should relieve the users of unnecessary chores.
   F. A system should provide for human information interface.
   G. A system should include provisions for corrections.
   H. Management should be held responsible for mismanagement.

2. Procedures for dealing with exceptions.

   A. A system should recognize as much as possible that it deals with different classes of individuals.
   B. A system should recognize that special conditions might occur that could require special actions by it.
   C. A system must allow for alternatives in input and processing.

D. A system should give individuals choices on how to deal with it.
E. A procedure must exist to override the system.

3. Action of the system with respect to information.

A. There should be provisions to permit individuals to inspect information about themselves.
B. There should be provisions to correct errors.
C. There should be provisions for evaluating information stored in the system.
D. There should be provisions for individuals to add information that they consider important.
E. It should be made known in general what information is stored in systems and what use will be made of that information.

4. The problem of privacy.

A. In the design of a system all procedures should be evaluated with respect to both privacy and humanizing requirements.
B. The decision to merge information from different files and systems should never occur automatically. Whenever information from one file is made available to another file, it should be examined first for its implications for privacy and humanization.

5. Guidelines for ethical system design.

A. A system should not trick or deceive.
B. A system should assist participants and users and not manipulate them.
C. A system should not eliminate opportunities for employment without a careful examination of consequences to other available jobs.
D. System designers should not participate in the creation or maintenance of secret data banks.
E. A system should treat with consideration all individuals who come in contact with it.

[This seemed worth drawing to your attention, although it might also be suited to Human-Nets and Soft-Eng. But to prevent subsequent discussion from wandering all over the place, let's see if we can constrain it to RISKS-related matters. Thanks. PGN]

Report problems with the web pages to the maintainer

Search RISKS using swish-e

THE RISKS DIGEST

Forum on Risks to the Public in Computers and Related Systems

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

Volume 4: Issue 45

Monday, 2 February 1987

Contents

DATE-86, or The Ghost of Tinkles Past

Rob Austein <SRA@XX.LCS.MIT.EDU>
Fri, 30 Jan 1987 00:48 EST

Extracted from the Arpanet-BBoards archives. --sra [NOTE DATES...]

Date: Wednesday, 11 December 1985 09:55-EST
From: Dan Hoey <hoey@nrl-aic.ARPA>
To: ARPANET-BBOARDS@MIT-MC.ARPA
Re: Software alert: DATE-86
ReSent-date: 14 Dec 1985 03:05:52 EST
ReSent-from: Arpanet-BBoards-Request@MIT-MC.ARPA

Early this year a message appeared on ARPANET-BBOARDS commemorating the ten-year anniversary of DATE-75. A somewhat more ominous anniversary will occur in four weeks, on 9 January 1986. Users of the TOPS-10 operating system should beware of software failures beginning on that date.

DATE-75 is the name of a set of program modifications applied to the TOPS-10 operating system, running on DEC PDP-10 computers. Before the modifications, the TOPS-10 system could only represent dates between 1

January 1964 and 4 January 1975. The DATE-75 modifications added three more bits to the representation of dates, so that dates up to 1 February 2052 could be represented. To maximize compatibility with existing software, the three extra bits were taken from several unused positions in existing data structures. The change was announced in mid-1974, and several tens of person-years went into updating software to recognize the new dates.

Unfortunately, reassembling these bits into an integer representing the date was somewhat tricky. Also, some programs had already used the spare bits for other purposes. There were a large number of bugs that surfaced on 5 January 1975, the first day whose representation required the DATE-75 modification. Many programs ignored or cleared the new bits, and thought that the date was 1 January 1964. Other programs interpreted the new bits incorrectly, and reported dates in 1986 or later. Date-related program bugs were frequent well into the Spring of 1975.

On 9 January 1986, the second bit of the DATE-75 extension will come into use. Users of software developed in the 60's and early 70's on the TOPS-10 operating system should beware of problems with testing and manipulation of dates. Beware especially of programs that were patched after manifesting bugs in 1975, for in the rush to fix the bugs it is possible that some programs were modified to assume that the date was between 1975 and 1986. Any date that is off by a multiple of eleven years and four days is probably caused by this type of bug.

Dan Hoey

Computerised Discrimination (an update)

Brian Randell <brian%kelpie.newcastle.ac.uk@Cs.Ucl.AC.UK>
Fri, 30 Jan 87 09:57:00 gmt

Since my original posting on this I've received enquiries as to whether there has been any follow up in the UK press. I hadn't seen any until today's Guardian, which carried the following (excerpted) article:

> MEDICAL SCHOOL FACES RACE INVESTIGATION
> By Andrew Veitch, Medical Correspondent
>
> The Commission on Racial Equality is to launch an investigation into discrimination against blacks at one of Britain's leading medical schools, it was disclosed yesterday.
> Sir Peter Newsam, the CRE Chairman, is invoking its rarely used legal powers under the Race Relations Act to investigate the way in which St George's in south London selects its students.
> This means that CRE officers have satisfied the commission that there is prima facie evidence that the Act has been breached. [...]
> The inquiry follows the Guardian's disclosure last month that the school was using a computer programme which deliberately downgraded non-white applicants.
> Two of its consultants, Dr. Aggrey Burke and Dr Jo Collier, ran applications through the computer and found that being a non-Caucasian female lowered the applicant's ranking by up to 20 points - probably enough to reject a candidate

who would have been accepted on academic performance alone.
The programme was designed to mimic the decisions of the selection committee, which it replaced.
The academic board scrapped the programme after being given details of the consultants' investigation.
...

Brian Randell - Computing Laboratory, University of Newcastle upon Tyne
UUCP : <UK>!ukc!cheviot!brian
JANET : brian@uk.ac.newcastle.cheviot

Another non-malfunctioning alarm

Jeffrey Thomas <Ad.JDThomas@CU20B.COLUMBIA.EDU>
Mon 26 Jan 87 17:56:45-EST

Garnered from a report just now heard on NPR's All Things Considered:
BBC reporter speaking of the investigation of the crash of the
airliner carrying Mozambique President Samora Machel:

> Based on official transcripts of the cockpit conversation before the crash, when a ground proximity alarm sounded, the (soviet) pilot ignored the alarm, believing it to be malfunctioning. The investigation also noted evidence that some of the instruments appeared to have been tampered with after the crash, fueling speculation by the soviets that the plane had been lured to the site by a false navigational beacon.

Re: Engineering models applied to systems, RISKS-4.42

Joseph S. D. Yao <hadron!jsdy@seismo.CSS.GOV>
31 Jan 87 02:42:57 GMT

I think that the concept of loosely-coupled systems can be very well applied to software engineering, although perhaps not in the way Wexelblat quotes Meldman as saying. There, the model seems to be that computer systems as a whole don't communicate well, and therefore prevent massive "data rot," as it were. That's as may be, and I may be reading it wrong anyway. But I see this as a very good model for the kinds of things we do in modularisation of software, information hiding, defensive programming, and the like. We try to make sure that errors in one part of a system don't propagate to other parts, by building bridgeheads against them (testing for bad data), not tightly coupling data values (controlling import and export), et alii.

Joe Yao hadron!jsdy@seismo.{CSS.GOV,ARPA,UUCP}
jsdy@hadron.COM (not yet domainised)

Re: A scary tale--Sperry avionics module testing bites the dust?

D. W. James <vnend@ukecc.uky.csnet>

28 Jan 87 00:47:42 GMT

>From: Nancy Leveson <nancy@ICSD.UCI.EDU>
> According to my FAA source, the FAA is not
>thoroughly comfortable with this, but the autopilot is only flight-crucial
>on this aircraft during about 45 seconds of the landing. Also, their tests
>have found that pilots can successfully recover from an autopilot failure
>during this period (by performing a go-around) about 80% of the time.

While not a direct computer risk, is anyone else troubled that
the FAA considers a 1 in 5 chance that the pilot WON'T recover acceptable?
Or is it just that they believe a failure during these crutial 45 seconds
to be of acceptably low probability?

UUCP:cbosgd!ukma!ukecc!vnend; or vnend@engr.uky.csnet; orcn0001dj@ukcc.BITNET

Search RISKS using swish-e

THE RISKS DIGEST

Forum on Risks to the Public in Computers and Related Systems

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

Volume 4: Issue 46

Monday, 8 February 1987

Contents

TV-program on PBS: NOVA - Why Planes Crash

Werner Uhrig <CMP.WERNER@R20.UTEXAS.EDU>
Tue 3 Feb 87 23:18:43-CST

I just saw this program tonight on the local PBS-station here in Austin, TX and would like to call your attention to it, as it may air later in your area (or as a daytime repeat later this week, as here in Austin).

It contained the most up-to-date and reasonable analysis and report of airline crashes in recent years I am aware of. It points out that human errors (mostly by the pilots) are the leading factors of these accidents and it reports on the programs major carriers have currently in operation

that try to reduce this (mainly having to do with Flight Deck Management and Human Factors in the cockpit).

One item that I found particularly interesting was a statement to the effect that the Automatic Pilot may well have been a contributing factor in several incidents, as the crew tended to trust the "computers" to the point to where they neglected to monitor the flight situation sufficiently and avoidable fatal accidents were the consequence. Examples included the case of a Chinese airliner crossing the Pacific on Auto-Pilot were one engine went out and the crew seemed not to notice in time to avoid entering a 6-mile, near-fatal dive, the crash of a liner near Miami, where the crew was occupied trying to analyze a burnt-out light-bulb of the "gear-down indicator", flying the plane on auto-pilot, unaware that, for reasons unknown, it did not hold the 2,000 feet altitude, even ignoring the warning buzzers until a few seconds before the end in the Everglade swamps. The shooting-down of the Korean airliner was also cited as an event were an incorrect data-entry and sloppy supervision procedures may have been the beginning of the end.

Re: TV-program on PBS: NOVA - Why Planes Crash

<MHARRIS@G.BBN.COM>
6 Feb 1987 14:21-EST

Some comments on "Why Planes Crash":

The program is not without virtues. But it suffers from the same sort of inaccuracies, omissions and misrepresentations seen frequently in such unthinkable contexts as recent New York Times articles, and will probably do further damage to the image of aviation.

Example: "Most accidents are caused by Pilot Error." Pilot Error is often a NTSB euphemism for "we don't know what happened." In fact, the last episode of the program, concerning the Delta L-1011 accident in Dallas, makes the points that NTSB decisions are often driven by politics, not safety per se, and that in this case "Pilot Error" was added to the causality findings of weather and controller/radar operator negligence so as to allow a "unanimous" decision to be announced -- leaving even my elderly parents wondering: if the microburst was so severe as to be unflyable (according to NCAR's McCarthy), and if its potential presence was not reported by the only people who could have known about it, how could it be the pilots' fault? "Too bad about the pilots' reputations, but we gotta look good on camera..."

The program did little to assure me that anyone out there understands the real problems and their possible solutions: too few competent controllers, failure to adapt useful technology (like Geostar-based position monitoring for collision avoidance), and FAA policies clearly dictated by political motives (e.g., the desire to control ALL airspace from the ground, thereby maximizing the FAA employee count & budget).

It would have been nice to see the point made that 1986 was one of the safest years EVER for U. S. aviation. 'Nuff said.

-- Michael Harris CFI

Electronic steering

Steve McLafferty <ssm%munsell.UUCP@talcott.HARVARD.EDU>
Wed, 4 Feb 87 12:02:50 EST

I, like many other readers of this forum, have become concerned about the increasing use of computers in our automobiles. I wonder about the increasing number of cars whose idle speed can go crazy due to a software bug. I have my doubts at times as to whether anti-lock brake systems are really failsafe, as their makers allege.

However, this week my concerns have turned into outright fear. Featured in the cover story of the February 2, 1987 issue of _AutoWeek_ magazine is a show car made by Pontiac, called the Pursuit. Unlike most cars made for auto shows, which are mostly exercises in styling, the Pursuit is a fully functional concept car. It features such goodies as full-time all wheel drive, active suspension with adjustable ride height, CRT instrumentation, etc.

The killer (pun intended) is the electronic four-wheel steering. There is no mechanical connection whatsoever between the steering wheel and the steering gearboxes! Two 24 volt battery-powered electric motors are responsible for turning the front and rear wheels. The article only mentions "electronics" for control, but presumably a microprocessor is involved. It is Pontiac's intent that many or all of the features of the Pursuit be incorporated in production vehicles by sometime in the 1990's, including the "steer-by-wire" system.

Steven McLafferty Eikonix Corp Bedford, Mass (617) 663-2115 x468
{{harvard,ll-xn}!adelie,{decvax,allegra,talcott}!encore}!munsell!ssm

Article: Senior to Repay Bank 25,000 Dollars

Steve Thompson <THOMPSON@BROWNVM>
Wed, 4 Feb 1987 13:10:31 EST

An article in the Feb. 2, 1987 Brown (University) Daily Herald (Providence, RI) describes an incident in which a Brown senior's account was "accidentally credited" 25,000 dollars last September by Citizens Bank located in Providence.

The article continues with information credited to the Providence (RI) Journal: (I have deleted the student's name.)

> According to the *Journal*, bank officials gave police the following account of the events: Approximately $4,000 was wired to [the student's] account on September 3. At about the same time, the bank said, $25,000 came into another customer's account. Due to an accounting mistake, the $25,000 was accidentally credited to [the student's] account.

The student claimed he thought his parents had wired the large amount of money to him. If he returns the amount, police will 'probably' drop all criminal charges. The student has spent a large portion of the money, but he said that he still planned to repay the bank.

I wondered what the phrase "accounting mistake" might mean, so I called Citizens Bank to see what I might learn. (I also wanted to give them a chance to give their side of things for this posting.)

As might be expected, a bank official was not excited about going into any detail about their mistake. I spoke with someone in (computer?) Security, who was very hesitant about speaking with me. All he would say was that if I thought the problem was computer-related, I was "heading in the wrong direction".

There is, as yet, no evidence that the error *was* computer-related, but "account mistake" is so vague that I can't help worrying...

And then there is the question of whether using money that you have been mistakenly given is illegal or not, and why. But best not to discuss that here, I guess...

Steve

Recursive risks in computer design

<Pavel.pa@Xerox.COM@MIT-CCC>
4 Feb 87 13:48 PST

Date: Tue, 3 Feb 87 16:27:34 PST
Sender: Swinehart.pa
From: McCullough.pa
Subject: Praise or attack?
To: Whimsy^.x

Open-Apple, Feb '87 mentions a Wall Street Journal article...

Recently, Apple Computer Inc. purchased a $14.5 Cray Research supercomputer to aid in the design of their next-generation Apple computers.

John Rollwagen, Cray Research Inc. chief executive, told Seymour Cray about how Apple was using their newly purchased Cray supercomputer. "There was a pause on the other end of the line, and Seymour said `That's interesting, because I'm designing the next Cray with an Apple.'"

Library Failure

<Chuck.Weinstock@sei.cmu.edu>
3 Feb 1987 10:05-EST

On Sunday CMU's computer center was shutdown due to an electrical

failure. The failure was bad enough that power was not restored to the building until sometime on Monday. Workers in that building were sent home until Tuesday.

The CMU library has totally computerized its catalog. This is really neat because it lets me search for books and other goodies from my office instead of trekking over to campus for nothing.

On Monday, of course, the library catalog was not operational. A talk with the reference librarian confirmed my fears: the card catalog has not been kept up to date and, in fact, will eventually be discarded.

I wonder if the power failure will convince them not to put all their eggs in the computer basket?

CP-6 time warp update (the true story)

<PHiggins@UCIVMSA.BITNET>
Tue, 3-FEB-1987 10:27 PST

I received a phone call from John Joseph at Honeywell's Los Angeles Development Center (the home of CP-6) yesterday. He clarified some points about my recent posting about the problem with the Front End Processor (FEP) Universal Time Stamp (UTS). I asked him to send me a written explanation to ensure that I got the facts straight.

I apologize if it appeared that I was criticizing Honeywell or its employees. During my time at Honeywell LADC, I found the staff there to be very competent and concerned with customer satisfaction.

Paul Higgins, Computing Facility, University of California, Irvine
phiggins@UCI.BITNET phiggins@ics.uci.edu

Here's John Joseph's message, in its entirety:

> Not to slight your mention of, and interest in, the "signed UTS" problem, I do have a minor correction to make to your analysis of the underlying problem. Your RISKs BB entry states something akin to: "the UTS word appears to have been declared as a signed number rather than an unsigned one". While that may be an obvious conclusion, based on the symptoms, it is not necessarily true, and casts doubt on the competence of the responsible programmer. The programmer did indeed declare the UTS as an unsigned value. The CP-6 host-based cross compiler that generated the code for the FEP generated what it could for the CP-6 FEP, namely, signed instructions, since the extended arithmetic mode of the CP-6 FEP can only do signed instructions. It generated these instructions without actually generating a diagnostic (warning) message for the programmer. E.g. the programmer probably thought he was doing it "right". In fact, all the criticism at the development center focused on the apparent oversight of the compiler programmer (which had its defendants, too). As a side note, the FEP could probably have executed some instructions to handle this situation properly, had Honeywell required its users to purchase a "Scientific Instruction

Processor" (functionally equivalent to an 8087 upgrade for a PC), at $3000. At that price, it's generally less than 5% of a total FEP purchase. Rather than force that upgrade, a decision was made to use the existing "Commercial Instructions Processor" (CIP) for extended airthmetic. With the unfortunate, but obvious results.

So, just to correct the record, I know the UTS problem was NOT a problem of a programmer declaring a datum incorrectly. There are a myriad of other, insidious, underlying problems that contributed to that appearance.

Dave Taylor <taylor%hpldat@hplabs.HP.COM>

t3b%psuvm.bitnet@wiscvm.wisc.edu, risks-request@sri-csl, jlarson@xerox
Date: Wed, 4 Feb 87 17:49:07 PST
Subject: Glitch in the Computers and Society Digest mailing list...

Last week while I was in Washington D.C. for a conference my "/usr" disk crashed and destroyed all the data on the disk. This unfortunately included the entire mailing list for the Computers and Society Digest, so I now have stuff to mail, and no-one to mail it to!

If you were on the list, or if you're interested in joining, please send me mail so I can rebuild it. Furthermore, if you know of any friends or others that were receiving the list...

(I remember having company burst points for BBN, SRI, Xerox, CMU, and some others, but not the actual addresses.)

This is all very frustrating, as you might suspect, so a slight sense of humour during this rebuilding process would be greatly appreciated too!

-- Dave Taylor

reputed moderator of The Computers and Society Digest

More on British Phone fraud

Will Martin -- AMXAL-RI <wmartin@ALMSA-1.ARPA>
Tue, 3 Feb 87 15:22:16 CST

Just as a brief followup to the recent discussions of British PhoneCard toll fraud, I heard a news item on a BBC World Service "News about Britain" program a couple days ago that a number of the staff at British Telecom have been charged with complicity in a toll-fraud scheme. This was only a sentence or two, giving no detail, but the fraud seemed to be plain human criminality, with no computerized aspects. Included amongst those charged were some operators; it appeared that the fraud was simple actions like not reporting for billing calls the operators handled. Perhaps someone on the list(s) with access to British media can post more details.

Regards, Will Martin

Wall Street Journal article on Risks

Jerome H. Saltzer <Saltzer@ATHENA.MIT.EDU>
Tue, 3 Feb 87 10:20:32 EST

The East Coast edition of the Wall Street Journal, on Wednesday January 28, 1987, contains a front page leader article headlined "As Complexity Rises, Tiny Flaws in Software Pose a Growing Threat." ... Most of the examples reported in the article have already appeared in Risks, but as a summary report to a wider audience, it is quite readable.

If you look for the article any place but the East Coast edition, be warned that different editions of the WSJ often run leader articles on different days.

Jerry

Search RISKS using swish-e

Report problems with the web pages to the maintainer

Search RISKS using swish-e

THE RISKS DIGEST

Forum on Risks to the Public in Computers and Related Systems

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

Volume 4: Issue 47

Monday, 16 February 1987

Contents

The fielding is mutuel!

Peter G. Neumann <Neumann@CSL.SRI.COM>
Mon 16 Feb 87 10:48:53-PST

On Tuesday, 10 Feb 87, Golden Gate Fields opened its 41st season racing season with a $3 million upgrade -- including its computer systems. Unfortunately, the first day was a disaster.

Due to starkly degraded computer capacity, only 80 of the 130 betting windows could be opened, despite adequate personnel for manning all windows.

And those 80 were operating at a snail's pace. Bettors waiting in line for 20 minutes never got their bets in.

The new Z Alpha Display next to the totalisator board was showing ridiculous probable payoffs. Actual payoffs could not be displayed and had to be announced.

The Pick Six had to be cancelled altogether. It, a new Pick Nine, and a daily triple all used computer-readable marked cards, but the equipment was not up to the task.

The GGF president Kjell Qvale said the reason for the breakdown was that the new equipment had been standing idly for too long and wasn't tested properly. Actually, mutuel machines are linked in groups of 8, and when one goes all 8 go. Something like 6 grids of 8 all collapsed. The resulting degradation in performance was intolerable.

this is another example of the difficulty of testing a system adequately without the presence of LIVE operating conditions... although it sounds as if they had plenty of time to do less-than-live testing...

[Derived from the SF Chron green pages, 11 Feb 87.]

Another worm story

Dave Platt <dplatt@teknowledge-vaxc.arpa>
Fri, 13 Feb 87 14:42:36 PST

There's a very interesting letter in the 1/87 issue of Byte magazine (page 408). Seems that the writer purchased a "speed-up BIOS chip for PC compatibles made by Softpatch Inc.", and installed it in his Televideo 1603 computer. Because the 1603 isn't strictly a PC-clone, he had to change two bytes in the video parameters (to suit the characteristics of the 14-inch monochrome monitor), and had to change one other byte to to make the BIOS checksum come out to zero. He decided to use the manufacturer's-logo byte for this latter change. Woe was he! The new BIOS contains a logo check, buried in the clock-tick interrupt routine, which is activated several hours after bootup. If the logo doesn't match, a glaring "PLEASE POWER OFF OR YOUR DISK WILL BE TRASHED!" message appears on the monitor, and if any key is typed (or is being held down when the message appears) the disk is "totally wiped out".

The writer reports that the documentation which comes with the BIOS chip makes no mention of the worm. He apparently spoke with the author of the BIOS, who told him that his choice of the logo-byte for checksum fudging was "unfortunate", and that he (the BIOS's author) had wiped out his own hard-disk twice while testing the worm.

Sounds to me as if Softpatch Inc. may be in a VERY dubious legal position with this worm, under the legal doctrine of "strict liability"... especially if the worm is accidentally activated on

someone's computer due to a "wild branch" into the BIOS, as the writer suggests might happen.

Re: The student's extra $25,000

Ronald J Wanttaja <hplabs!cae780!tektronix.TEK.COM!uw-beaver!ssc-vax!wanttaja@ucbvax.Berkeley.EDU>
Fri, 13 Feb 87 09:56:57 pst

At a recent aviation safety conference, Jack Eggspuler told a story similar to that of the student with the extra $25,000 credited to his account [Steve Thompson, RISKS-4.46]:

He had banked for years at a small-town bank. One day, a large banking conglomerate bought up the small bank. After this, Jack noticed that his deposits weren't being listed.

He went into the bank to talk to them. It turned out that his account number, which had been assigned to him when the bank was independent, was identical to Borden Industries' account number with the conglomerate. Yup, his penny-ante deposits were going into Borden's account.

He thought it was straightened out. A week or so later he went in to cash a check, and asked for his balance. It was: $9,238,345.35. Ulp! He thought of a new Piper, but settled for a copy of the printout. He's got it hanging on his wall...

GIBU: Garbage in, Bucks out?

Ron Wanttaja (ssc-vax!wanttaja)

Problems with the B-1B Bomber

Bill McGarry <decvax!bunker!wtm@ucbvax.Berkeley.EDU>
Wed, 11 Feb 87 0:15:16 EST

In the January 19th, 1987 issue of Newsweek, there is an article on the problems with the B-1B bomber project (page 20) . Three key systems are reported as being "faulty" with two of those attributed to software problems:

* Terrain-following radar: "Software glitches have prevented pilot training but Air Force engineers say the flaws will be corrected within weeks."

* Flight-control software: "..is especially critical during delicate in-flight refueling operations. Faulty software programs make such operations difficult."

The third key system, electronic countermeasures systems (stealth), is reported as "jamming their own signals instead of the enemy's" but it was not mentioned whether software played any role in the problem.

Bill McGarry, Bunker Ramo, Shelton, CT

PATH: {philabs, decvax, ittatc}!bunker!wtm

Super-Smart Cards Are Here.

Leo 'Bols Ewhac' Schwab <well!ewhac@lll-lcc.ARPA>
Wed, 11 Feb 87 23:30:58 pst

I just saw an article in the San Francisco Chronicle describing a new little goodie which inventors have called the Super-Smart card. It is a credit-card-sized unit with lots of memory in it, and it also appears to have a 12-key keypad on the back.

What I found interesting about this article is that its inventors don't know what to do with it (solution looking for a problem), and are soliciting potential applications, such as encoding medical information.

Do we really need this? Think about it. Supposedly "foolproof" systems have been defeated before (VideoCypher, British Telecom, countless computer systems, etc.). Why should this be any different?

This is not just a card with an indentification number specially encoded, this is a full computer system in a credit card. It's got memory, I/O, an external interface (I would surmise that this would be the case so external readers can be plugged in), etc. Imagine: All your personal information encoded on a credit card.

What if it's stolen? Thieves are getting more and more ingenious, and a particularly smart one could easily upload all the information out of the card. What if an even more ingenius person encoded fabricated information on the card?

Suppose you're in an auto accident. The card is damaged. How will emergency personnel read the vital medical information?

The list could go on. I agree that it's a neat gadget, and wouldn't mind having all kinds of information available in my wallet, but do we REALLY need something like this? Not necessarily because of the RISKS involved, but just as a new piece of technology to worry about.

"Damn, the batteries are dead. And I can't buy new batteries without the card. And I can't use the card because the batteries are dead..." :-)

Leo L. Schwab ihnp4!ptsfa!well!ewhac
well ---\
dual ----> !unicom!ewhac
hplabs -/ ("AE-wack")

Iranamok Computer-Databased

Craig Milo Rogers <Rogers@venera.isi.edu>
Thu, 12 Feb 87 09:21:32 PST

From the Los Angeles Times, Wed 11 Feb 1987, front page:

> IRAN INQUIRY REPORTED FOCUSING ON NEW DATA
>
> ... Computer Records Revealed
>
> ... FBI agents reviewed National Security Council computer records ...
>
> The records, part of a massive electronic filing system disclosed to investigators by the White House this winter, contains copies of private messages sent between National Security Council offices to the White House's internal IBM computer network, called PROFS. ...
>
> The computer messages under scrutiny by the FBI - which range from routine memos and obscene jokes to eyes-only accounts of intelligence operations - were composed and sent by most NSC employees in the belief that they were not being recorded elsewhere.
>
> In fact, however, their contents were stored on magnetically treated "hard" computer discs and retained for at least one to two months before being erased, White House spokesman Dan Howard said Tuesday.
>
> "We were living under a delusion. We thought when we deleted them from our own files, that they dissapeared," the rueful Administration official said. "In fact, they were just going into storage." ...
>
> The rest of the article contains more details on who was using the system and what they were saying.

Craig Milo Rogers

Re: Electronic steering (RISKS-4.46)

<ulysses!gamma!pyuxww!sw1e!uusgta@ucbvax.Berkeley.EDU>
Tue, 10 Feb 87 22:05:01 est

Lear Jets have no mechanical connection between rudder pedals (steering wheel) and nose wheel. I would also assume a microprocessor is involved. While I have seen these jet's steering fail (intermittently) due to water leakage I have never heard of an accident attributed to this. This lack of steering linkage means the nose wheel swivels freely without power (*very* helpful to linesmen). It is probably useful to note that main wheels are independently brakeable though.

---Tom Adams---

{bellcore,ihnp4}!sw1e!uusgta St. Louis MO 314-235-4237
Opinions expressed here are mine, not those of Southwestern Bell Telephone

---

Re: Electronic steering

Amos Shapir <decwrl!nsc!nsta!instable.ether!amos@ucbvax.Berkeley.EDU>
Wed, 11 Feb 87 08:49:10 -0200

In RISKS-4.46 Steve McLafferty writes:

>The killer (pun intended) is the electronic four-wheel steering. There is
>no mechanical connection whatsoever between the steering wheel and the
>steering gearboxes!

I really hope that scheme never makes it to production! Last time I heard,
power steering and brakes are designed in such a way that even when all power
is lost, the driver can still control the car and stop manually.

  Amos Shapir
National Semiconductor (Israel)
6 Maskit st. P.O.B. 3007, Herzlia 46104, Israel
(011-972) 52-522261 amos%nsta@nsc.com 34.48'E 32.10'N

Re: Nova: Why Planes Crash (RISKS-4.46)

Alan M. Marcum <marcum%nescorna@Sun.COM>
10 Feb 87 17:30:51 GMT

In RISKS DIGEST 4.46, Werner Uhrig wrote:
 >I just saw [Nova: Why Planes Crash].... One...interesting [item] was...
 >that the [autopilot] may... have been a... factor in several incidents....
 >Examples included...a Chinese airliner...[where] one engine [failed]...

I've read the NTSB report on this incident (and I saw the television
program). It appears to have been much more a case of pilot error
(failing to follow standard procedures -- namely "disengage the autopilot
upon engine failure") than of "computer failure."

 >...the crash...near Miami, where the crew was occupied trying to analyze a
 >[lack of gear-down indication], flying the plane on auto-pilot, unaware
 >that...it did not hold [2000']....

Again, this was much more a disregard of primary duties: no one bothered to
fly the airplane. Three supposedly qualified pilots all diverted nearly
their entire attention from their primary jobs at the same time, for several
minutes!

Now, do these (and others) indicate an over reliance on technology? Is THAT
the risk we're seeing in aviation today? Or is it lack of sufficient
training in systems that are growing more and more complex? During primary
training and initial instrument training, a good curriculum will include

tremendous information about the systems of the aircraft. A frequent criticism of recent airline training is that it is becoming more procedures-based ("if this happens, do this"), rather than systems-based ("this is how it all works, and plays together").

As a counterpoint (i.e. that in many cases it IS an error on the part of the pilots -- often an error which adherence to procedures, even as taught in procedures-based training, could have avoided), during the China Air incident, the entire cockpit crew, including the backup crew, experienced severe spatial disorientation. Everyone there misinterpreted the attitude indicators (one of the primary non-visual flight instruments, used in essentially every instrument-capable airplane, from trainers like Cessna 172s, to 767s and L1011s), which showed, very clearly, and correctly, what was happening to the 747 as it began its uncontrolled (though NOT uncontrollable!) roll. Both the captain and the first officer believed that both of their attitude indicators (attitude indicators in that 747, and in most planes, are gyroscopic instruments) had tumbled at the same time! As soon as the plane broke out below the clouds, the captain was able to recover from the unusual attitude -- using VISUAL flight skills.

How much of the China Air incident could be blamed on computers? On technology? On training? Where are the REAL risks?

Alan M. Marcum Sun Microsystems, Technical Consulting
marcum@nescorna.Sun.COM Mountain View, California

Re: Library computerization

Will Martin -- AMXAL-RI <wmartin@ALMSA-1.ARPA>
Wed, 11 Feb 87 9:34:08 CST

The St. Louis Public library has also recently eliminated its physical card catalog and gone to a computerized system for cataloging and for book loaning and tracking. It is based on bar-code scanning, and I've noticed a rise in incorrect book-overdue notices and the like; one specific example that happened to me was that I had checked out and returned a book which had water damage distorting the bar-code label. Some weeks after returning it I got an overdue notice, so I went to the library, found the book on the shelf, and took it and the notice to circulation to remonstrate with them. They seemed to be used to reports of errors by that time, so I suppose this was relatively common. My guess for the reason for that error was that the bar-code-reader returned an incorrect reading when they processed the return.

This was during their transition period, though, and things seem better now. However, the catalog is now on microfilm or -fiche, which is harder to use than the paper card catalog, plus it is only updated periodically. (With the paper cards, they could always insert new cards at any time -- whether they actually DID this, or waited until they had a batch to put in, or did it on a weekly or other time-based schedule, I do not know.)

I find the COM microfilm catalog to be particularly difficult to use,

as the film is in manually-driven reader units, and there is no
indication to the user just where in the reel the viewer is pointing.
(That is, they have the author/title and subject catalogs both on
the same reel, and I can never remember which is first, and they do not
tell you. So you turn on the reader and see you are looking at "M" in
the author/title section, and you want to go to "G" in the subject
section. You have to crank for a minute or so in one direction and hope
you are going the right way; if not, you hit end-of-reel, and have to
crank back over what you already skipped over, plus the rest of the
alphabet, before you even get into the section you want to search.)
At least the fiche allow a random or direct search to get the right
fiche, and then you can jump around within it with the reader unit.
But you always have to look at two fiche -- they issue change-update
sets more often than they re-issue a complete updated catalog set.

Regards, Will Martin

Second British Telecom Fraud

"Lindsay F. Marshall" <lindsay%kelpie.newcastle.ac.uk@Cs.Ucl.AC.UK>
Tue, 10 Feb 87 09:39:20 gmt

This had nothing to do with the Phonecard scam. As far as I could make out
from the newspaper reports it was a simple fraud - probably worked by
hacking wiring in exchanges or something (that is a pure guess, no details
were mentioned). There certainly seemed to be no computer aspects involved.

Lindsay

P.S. Does anyone have a pointer to the work on human error being done by people
at UCSD? Hofstadter mentions it in his latest book and it sounds interesting.

Search RISKS using swish-e

THE RISKS DIGEST

Forum on Risks to the Public in Computers and Related Systems

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

Volume 4: Issue 48

Wednesday 18 February 1987

Contents

Four near air misses in 1986

"Lindsay F. Marshall" <lindsay%cheviot.newcastle.ac.uk@Cs.Ucl.AC.UK>
Wed, 18 Feb 87 10:11:29 GMT

From the Observer 15th Feb 87:

17 March 86. A crowded One-Eleven jet and a Short 330 commuter aircraft descend to land simultaneously on Aberdeen's single runway. The jet screams over the top of the slower plane, cuts through its descent path, then aborts landing, narrowly averting catastrophe. An Aberdeen radar controller is blamed.

28 November 86. An Iran Air jumbo jet is told to stay at 6,000ft but instead climbs and almost collides with an Air UK Fokker F27 in holding stack over Heathrow. The Iranian crew's poor English makes analysis of the incident impossible.

13 December 86. Over Detling, Kent, a Britannia Airways 737 from Luton to Munich comes within half a mile of a One-Eleven bound for Amsterdam from Gatwick. The controller handling 14 aircraft simultaneously, had forgotten the 737's existence.

22 December 86. A British Midland One-Eleven en route from Heathrow to Leeds is instructed to climb to 28,000ft. Over Cranfield, Bedfordshire, it passes a United States Air Force KC135 tanker aircraft crossing the airway at the same altitude. The pilot of the passenger jet takes evasive action. A trainee controller had forgotten the presence of the military jet.

Radar failure (From the Observer 15th Feb 87)

<"Lindsay F. Marshall" <lindsay%cheviot.newcastle.ac.uk@Cs.Ucl.AC.UK<>
Wed, 18 Feb 87 10:11:58 GMT

At 6.30 a.m. on 15 November 1986 the London Air Traffic Control Centre (LATCC) at West Drayton suffered a total loss of main power as the morning rush of flights began. A standby generator also failed. Radar screens covering Wales and England south of Newcastle went blank. The IBM 9020 computer shut down, halting updating of flight progress strips. Controllers had to revert to writing strips manually.

Radio contact with aircraft was precariously maintained by a battery supply with a life of 30 minutes. Pilots continued to fly in the busy airspace without radar by scrupulously maintaining their separation from other planes. But without radar monitoring by controllers on the ground little could have been done if a jet had strayed.

Power was restored five minutes before the batteries gave out. The fault was blamed on a freak sequence of events started by the failure of a small capacitor.

Managers were eager to clear the backlog of flights but the computer would not function normally. It displayed some radar blips but not others.

The LATCC controller said: 'We were pushed to handle more aircraft but refused because the computer could have gone down at any time.

'There were many near misses that morning, all due to equipment failures. We were lucky. If the same sequence of events occurs in the summer, the effect does not bear thinking about.'

Computer failure causes flight delays

<Hoffman.es@Xerox.COM>
18 Feb 87 08:06:35 PST (Wednesday)

Excerpted and edited from the Los Angeles Times, Feb. 15, 1987:

FLIGHT DELAYS LAID TO COMPUTER MALFUNCTIONING
By Dean Murphy

Flights from airports throughout Southern California were delayed during most of the day on Friday because of a 30-minute early morning computer failure at the Los Angeles Air Route Traffic Control Center at Palmdale, according to Federal Aviation Administration spokesman Russ Park. A backup system was activated 14 minutes after the outage.

The aging computer, known as the 9020, has been the source of numerous controllers' complaints, and is expected to be replaced later this year. It provides information abot the flight plans of aircraft over a 180,000-square-mile area of Southern California, southern Utah, southern Nevada and western Arizona. Palmdale controllers give flight instructions to pilots while they are flying above 10,000 feet between areas that are covered by controllers at individual airports. The 9020 failed 12 times during the last six months of 1986, with an average failure time of about four minutes.

The outage Friday forced air traffic controllers to ground flights for 15 minutes during the morning rush period at airports throughout the area. Combined with heavy air traffic and rainy weather, delays continued through much of the day. Airport and airline spokesmen said that most of the delays were minor, describing the situation as more of an irritation that a significant disruption in service. The outage posed no safety hazard to passengers. Controllers lost flight plan information -- including such things as the flight number, altitude and airline of each flight -- during the 14-minute transition to the backup system, but they were able to continue tracking the planes on radar screens.

-- Rodney Hoffman

Real RISKS (as opposed to virtual risks) of aircraft

Eugene Miya <eugene@AMES-NAS.ARPA>
Tue, 17 Feb 87 18:23:18 pst

Been some time since I've sent something in, but Alan Marcum brings up some good issues with respect to flying aircraft.

Alan brings up some good buzzwords like a systems approach to training. What does this really mean? You don't want a pilot doing "long-hand" reasoning as the plane is falling out of the sky. This is not to say they are reading paper when they are going down either.

Pilots get a systems approach (so believed right now), but it is not clear what they don't need to know. A friend at the MVSRF (featured in the Nova episode for NASA/Ames) pointed out in a local meeting at PARC a couple of months back that checklists are written in blood. (Obviously dramatic, but true.)

I have also learned in recent days that war gaming and battle management can be regarded as `batch' rather than `interactive' in nature. There are those local `interactive' things called "engagements," but good commanders set up battles months and weeks in advance to anticipate the widest variety of contingencies, and not to fight or fly "on the fly." This is part of why checklists exist. They are hardcopy versions of our memory. They don't forget, or suffer interference. We try to think of contingencies before they exist. Sure, they are hardwired, and have lots of problems, and there are people doing research on check lists here and other places.

Yes, if we get lax because of computers, this is a computer associated risk. The human factors people have done LOTS of work to differentiate knobs in planes. If we computer people fail to do a similar job with software (as an example), then we will kill people.

--eugene miya, NASA Ames Research Center

p.s. would you trust your life to any single line of code you wrote?
think about it, before answering. I've worked on flight (space) projects, but not man-rated, don't know if I could.

Trojan Horse alert (from mod.computers.ibm-pc)

<forags%violet.Berkeley.EDU@berkeley.edu>
Mon, 16 Feb 87 15:58:01 PST

... This one could be serious, given the popularity of PC-Write.
Al Stangenberger, Forestry, U.C. Berkeley

Date: Thu, 12 Feb 87 11:12:22 EST
From: "Peter J. Laughton" <PJL%MX.LCS.MIT.EDU@MC.LCS.MIT.EDU>
Subject: PC-Write Trojan Horse

In light of the announcement of PC-WRITE availability to Info-IBMPC readers (volume 6, issue 8), I considered that it would be valuable to share the following warning:

> ---
> TROJAN HORSE ALERT: BOGUS PC-WRITE 2.7x
> ---

The latest INFOWORLD (02/09/87) reports the discovery of a bogus version of PC-WRITE.

Tom Wilkinson, the sysop in Los Angeles who discovered it says "the trojan version when invoked, destroys the file allocation table of a user's hard disk, and initiates a low level format, destroying the hard disk's data."

The bad version pretends to be the latest version, PC-WRITE 2.71 and is 98,274 bytes long.

The real version of 2.7 is 98,242 bytes long, and the real version of 2.71 is 98,644 bytes. Wilkinson says the version posted on Compuserve is the real version.

INFOWORLD reports that "Quicksoft, PC-WRITE's developer, is offering $2500 reward for the first person who identifies the creator of the bogus program and a $5000 reward for the person who provides proof that convicts the perpetrator."

Don Richardson, 02/10/87

From: jam@mitre-bedford.ARPA

According to Quicksoft, the publisher of PC-Write, the latest version is 2.71. Version 2.72 is a hack containing a booby trap, and trashes hard disks. BEWARE!

Version 2.71 is a minor update of 2.7. They will not release a version 2.72. They are trying to notify bulletin boards of the existence of the bogus version, but are walking a thin line: they don't want to scare people away from PC-Write.

I use version 2.7 and like it a lot.

Joshua Morris, jam@mitre-bedford

``Computerized Town Data Vanish''

<LEICHTER-JERRY@YALE.ARPA>
16 FEB 1987 13:04:53 EST

(From the Sunday 15 Feb 87 New York Times)

Prescott Valley, Ariz., Feb. 14 (AP) -- All the computerized financial records of this Rocky Mountain community have been erased, leaving officials with no idea how much money has been spent this year or how much cash the town has left.

Mayor Phil Beeson told the Town Council on Thursday that the account shows a balance of zero.

He called it "positively a case of deliberate attack." Lyn Newton, assistant town clerk, said Friday that there is "strong circumstantial evidence pointing to one person" whom she would not identify.

Ms. Newton said she discovered the problem over the weekend as she began closing out the books for January for the town of 2,700 residents.

"All our expenditure accounts and all of our revenue accounts were erased," she said. "The thing that scared me so badly is that we have no valid means of knowing where we are. By the time this was discovered, we could have been way over budget."

The records apparently were erased sometime between Jan. 1 and last week, Ms. Newton said.

They can be reconstructed, she said, but the task will be time consuming and expensive and will be complicated by the fact that the town manager, assistant town manager and town clerk all left office in recent weeks.

And, she said, it is time to begin preparing next year's budget.

Re: UCSD work on human error (RISKS DIGEST 4.47)

Alexander Glockner <sdcsvax!beowulf.UCSD.EDU!glockner@ucbvax.Berkeley.EDU>
Mon, 16 Feb 87 23:12:23 pst

Regarding the UCSD work on human error mentioned in the last line of the most recent risks digest:

> Donald Norman (norman%sdics@sdcsvax.ARPA) is the
> investigator who has done the most work here on the subject.

Connector risk

Rob Horn <wanginst!infinet!rhorn@harvard.HARVARD.EDU>
Mon, 16 Feb 87 17:57:08 est

The growing popularity of using the RJ series connectors (aka `telephone modular jacks') for terminal cabling is exposing a lot of people to a major risk. These jacks are directly interchangable with normal telephone jacks, and you can be sure that people will make mistakes and plug terminals into telephone equipment. This can do tremendous damage, and may even pose a health risk.

When a telephone rings, the ring signals are a pulsed DC that can reach as high as 150 volts! In terms of vaporized semi-conductors, this is just as destructive as plugging your connector into an electric outlet. The frequency, voltage, and power don't quite match standard electric power but they are more than enough to totally destroy any unprotected electronics.

The health risk arises from the potentially poor grounding of the digital electronics. These circuits are not normally designed to be safe with 150 volts on them. This risk may be shortlived since the digital circuit will quickly self destruct. Telephone extension cables with RJ connectors pose a greater hazard. When the phone rings there is high voltage on that connector. If a child is chewing on it when the phone rings there is a real risk of death from electrocution. (The hazard to adults is lower since they don't normally chew on cables, and the power levels are low enough that the odds are in favor of a nasty jolt instead of fatal one.)

Beware of using these connectors in inappropriate circumstances. (I was warned quite thoroughly by our Mechanical Design people when I suggested it. I learned then for the first time that telephones are not UL approved, nor

will they ever be, because of this 150 volt risk.)

Rob Horn
UUCP: ...{decvax, seismo!harvard}!wanginst!infinet!rhorn
Snail: Infinet, 40 High St., North Andover, MA

[Amos Shapir: Re: Electronic steering]

Brint Cooper <abc@BRL.ARPA>
Tue, 17 Feb 87 9:30:06 EST

The following makes me wonder why no widespread concern exists about failure of "conventional" power steering and brakes when an auto engine dies. I have had both experiences, fortunately without accident, and they are frightening. If we haven't worried about that risk, will we collectively worry about the risk of an electronic system failure?

_Brint

> From: Amos Shapir <decwrl!nsc!nsta!instable.ether!amos@ucbvax.Berkeley.EDU>
> In RISKS-4.46 Steve McLafferty writes:

>The killer (pun intended) is the electronic four-wheel steering. There is
>no mechanical connection whatsoever between the steering wheel and the
>steering gearboxes!

I really hope that scheme never makes it to production! Last time I heard, power steering and brakes are designed in such a way that even when all power is lost, the driver can still control the car and stop manually.

Amos Shapir

Search RISKS using swish-e

Report problems with the web pages to the maintainer

Search RISKS using swish-e

THE RISKS DIGEST

Forum on Risks to the Public in Computers and Related Systems

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

Volume 4: Issue 49

Sunday, 22 February 1987

Contents

A misplaced report

<COHEN@C.ISI.EDU>
21 Feb 1987 17:56:29 PST

I enjoyed very much the interesting report by Lindsay F. Marshall (RISKS DIGEST 4.48) that shows four near-miss incidents in the UK. The reasons for the incidents are: (1) An Aberdeen radar controller, (2) The Iranian crew, (3) The controller who handled 14 aircraft simultaneously and had forgotten the 737's existence, and (4) a trainee controller who had forgotten the presence of the military jet.

I find this important report to be misplaced. It must belong to another RISKS-FORUM Digest, one that is not a "FORUM ON RISKS TO THE PUBLIC IN

COMPUTER SYSTEMS" like ours, but to the "FORUM ON RISKS TO THE PUBLIC IN MANUAL SYSTEMS".

I do not find it fair that we include their stories in our bulletin.

By the way, I guess that they had a field day with the train accident, the one in the East that none of us managed to blame computers for.

Danny.

[I HAVE INFORMALLY BEEN WORKING UNDER THE CRITERION THAT RISKS is a forum on risks to the public in COMPUTER-RELATED TECHNOLOGIES. If the computers in a computerized system are not used to proper advantage to prevent something that is caused by PEOPLE, that is relevant. If there are no computers in an environment that is critical (and especially if it is difficult to control), then that also is relevant. In the former case, the existence of computers often leads people to rely on the computer systems rather than remember that they (the people) are critical elements in the overall system. In the latter case, the absence of computers is itself an issue. Besides, it was a slow week otherwise. But, I left out the trains anyway... PGN]

Relevance

Amos Shapir <decwrl!nsc!nsta!instable.ether!amos@ucbvax.Berkeley.EDU>
Sun, 22 Feb 87 11:36:48 -0200

This is starting to become ridiculous. In RISKS-4.48 there were only 2 articles concerning computers; all the rest were about aviation, cars and telephones - nice horror stories, but all referring explicitly to human error (not while using/programming computers) and faulty hardware (not computer hardware). I thought the purpose of having this group moderated was to prevent such articles from filtering through! (Yes, I know, some of them are mine, I admit).

Amos Shapir, National Semiconductor (Israel)

Re: London ATC (RISKS-4.48)

<jhc@mtune.ATT.COM>
20 Feb 87 22:30:35 EST (Fri)

In RISKS Vol 4 Issue 48 Lindsay Marshall reproduces a recent news article from The Observer, which is a quality newspaper:

> London Air Traffic Control Centre ... suffered a total loss of main
> power as the morning rush of flights began.
> A standby generator also failed ...

Now, even allowing for paraphrasing and journalistic licence, it would seem to be relevant to ask what happened to the secondary and tertiary

main (grid) power feeds, the secondary and tertiary generators, the secondary battery system, and why the battery system was apparently only designed to last for 30 minutes. Phone switches have better backups! At least Bell Systems' ones do -- I can't speak for British Telecom. Of course these systems may have been the result of Government cost savings...

Jonathan Clark

Disk space cleanup causes problems with on-line Bar Admission exam

<mnetor!lsuc!dave@seismo.CSS.GOV>
Thu, 19 Feb 87 18:00:37 est

Here's a story about how a little innocent disk-space cleanup led to a student doing an exam, and being told he'd passed, when he shouldn't have been allowed to take it at all.

All law students in Ontario must pass the Bar Admission Course before they become lawyers. One course in the BAC is on Accounting in a Law Office. This course is taught by CAI, and the exam is on-line. Every student gets a different exam; the random seed is the student's (internal, numerical) user-ID on our UNIX system, so that we can easily reproduce any student's exam if need be.

Students who fail the exam on the first crack are allowed to do it again as a supplementary. They are supposed to get a new account installed for them and use the new account. With the new account, they get a different user-ID and therefore a different exam. If they try to use their original account to do the exam again, once they've already done it, the system stops them.

A student took the exam on a Tuesday afternoon and failed (scored 44%). He didn't contact us to get a new account set up, merely came in on Wednesday morning and took the exam again. Taking EXACTLY THE SAME EXAM, he scored 50% and was told he'd passed.

We discovered this when our weekly statistics run told us that out of 538 students who had taken the exam, 536 had passed and 3 had failed! (The Bar Admission Course's overall pass rate is very close to 100%. You have to be pretty bad to get 50% your second time round on the SAME exam!)

Normally the system would have prevented him from taking the exam again. However, in an effort to free up some disk space that Tuesday night, I combined all students' result files into one compendium. (There was a one-line file for each student account, and disk blocks were used much more efficiently by combining them all together.) I had forgotten that the way the system stopped a student from taking the exam twice was by detecting the existence of a result file! (This has been fixed.)

Also, the message to the student indicating that he had failed, but could retake the exam as a supplementary, did not indicate that he'd have to get a new account to do so. (Now it does.)

What we decided to do was contact the student and tell him that the allowing of him to retake the same exam was a mistake and he must do it again. Fortunately, he didn't object, took it again (different exam) and passed. If he had objected, I don't know what we would have done. How do you fail someone after he's taken an exam and passed?

David Sherman (dave@lsuc.UUCP), The Law Society of Upper Canada, Toronto

Automatic Call Tracing for Emergency Services

<MJackson.Wbst@Xerox.COM>
20 Feb 87 11:08:59 EST (Friday)

On February 4 a restaurant near Rochester, NY caught fire. The owner dialed 911, which connected him to the county-funded, city-run emergency services network. Apparently he told the operator that the fire was at "321 Linden Ave." The Automatic Location Indicator, a system which uses a computer file maintained by Rochester Telephone to identify the address from which incoming calls originate, displayed "321 Linden Ave. Brighton" [a suburb of Rochester]. Fire trucks were immediately dispatched to that address.

Unfortunately, the restaurant is located at 321 Linden Ave. in East Rochester, another suburb several miles east. Fortunately, about two minutes later the fire was called in by someone else who did specify the proper location; the additional damage suffered because of this delay does not appear to have been major.

Operators for 911 are instructed to seek locations from callers, and to rely on the ALI only when the caller is unable to give that information. In this case, however, it seems clear that in the absence of the ALI the operator would have attempted, almost certainly successfully, to ascertain the town involved orally. Thus the faulty data in the ALI file was the cause of the dispatching delay. It appears that such errors, while not common, are not extremely rare either.

(Incidentally, the county Commissioner of Public Safety took this occasion to complain about duplicate street names within the county, apparently a continuing sore point here. It strikes me that the system (computers and procedures) should be robust enough to handle this; after all, if one eliminated the duplicates one would still have the sound-alikes, numbers east versus numbers west, and so forth.)

Re: The student's extra $25,000

Kee Hinckley <apollo!nazgul@EDDIE.MIT.EDU>
Fri, 20 Feb 87 11:16:15 EST

> At a recent aviation safety conference, Jack Eggspuler told a story similar to that of the student with the extra $25,000 credited to his account

> [Steve Thompson, RISKS-4.46]:
>
> He had banked for years at a small-town bank. One day, a large banking conglomerate bought up the small bank. After this, Jack noticed that his deposits weren't being listed.

A similar thing happened to me through the Massachusetts Baybanks chain. Although it is it statewide bank it's actually split into smaller regional banks. I had/have an account Baybank/Middlesex. Unfortunately someone else had an account with Baybank/Harvard with the same individual account number (although the bank codes were different). Every few months she would make a deposit or (more often) a withdrawal at a Baybank/Middlesex branch and the teller wouldn't notice that the bank number was different. Bingo, money out of my account. After three such errors (including one that resulted in an overdraft), and a number of fights to insure that I got back all charges and interest, Baybanks finally agreed that something should be done about it - namely having me change my account number.

This is one instance where I'd far rather trust my account to a computer that reads ALL of the information off my banking card.

-nazgul

[See my comment after Danny Cohen's message above, especially if you don't think this should be relevant to the RISKS Forum! PGN]

Re: Electronic steering

"Hien B. Tang" <hbt@ICSE.UCI.EDU>
Fri, 20 Feb 87 10:47:43 -0800

> <> The killer (pun intended) is the electronic four-wheel steering. There is
> <> no mechanical connection whatsoever between the steering wheel and the
> <> steering gearboxes! Two 24 volt battery-powered electric motors are
> <> responsible for turning the front and rear wheels. ...

I don't see why just using electronic steering is dangerous. Especially in today's litigious society. I am sure that the car makers will think of this when they put the electronic control in.

Side note: Isn't the F-16 a fly-by-wire plane? If electronic steering is safe, and reliable enough for combat jets, why wouldn't it be safe enough for everyday car?

Re: TV-program on PBS: NOVA - Why Planes Crash

<pyramid!utzoo!henry%hplabs@hplabs.HP.COM>
Sun, 22 Feb 87 02:46:52 pst

> > ...leaving even my elderly parents wondering: if the microburst was
> > so severe as to be unflyable (according to NCAR's McCarthy), and if

> its potential presence was not reported by the only people who could
> have known about it, how could it be the pilots' fault? ...

They flew into/under what they clearly saw to be a violent thunderstorm. There are few worse sins in flying. Their only excuse was the the planes ahead of them had gotten away with it -- an attitude that has been loudly criticized in other contexts, e.g. the Challenger disaster.

Henry Spencer @ U of Toronto Zoology
{allegra,ihnp4,decvax,pyramid}!utzoo!henry

Re: RJ (phone) connectors for terminals

Jordan Brown <jbrown@jplpub1.uucp>
22 Feb 87 05:16:46 GMT

If you are going to use RJ parts for terminals, you should make the center wires (red and green) be ground, and tie them together in your RJ to DB25 box. If you plug this cable into a phone system it looks like a phone which is off the hook.

This is, of course, only true for single-line service, but that is probably the vast majority.

Properly wired RJ terminal cables solve just about all of the problems with RS232. You want to plug your terminal into your modem? Great, just use a standard male-male cable. PC into terminal? Same. PC into printer? Modem into printer? Terminal to terminal? Same. Solve the wiring problem ONCE for each device that comes in the door, and you never have to do any work to connect any two devices. If you'd like further info on how to wire like this, send mail.

This scheme (the one I'm familiar with, superior to all others I've seen) was developed (I believe) by Dave Butterfield at UCLA, and is used there. The parts are much smaller, cheaper, and easier to use than DB25s.

Search RISKS using swish-e

THE RISKS DIGEST

Forum on Risks to the Public in Computers and Related Systems

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

Volume 4: Issue 50

Monday, 23 February 1987

Contents

Principles of RISKS

"James H. Coombs" <JAZBO%BROWNVM.BITNET@wiscvm.wisc.edu>
Sun, 22 Feb 87 23:32:07 EST

I have been reading RISKS for a while now and find that I have absorbed some healthy principles. I recently developed a program that relies on coding to determine how to manipulate data. After completing the first version, I found that I had a much higher proportion of coding errors than expected. Since I do not want to proofread reports microscopically, I decided to rewrite the program to analyze the data automatically (as much as practical). I then considered doing away with the hand-coding altogether, but the RISKS of relying excessively on computer programs to determine the "right results" quickly came to mind. The second version of the program uses the results of its own data analysis, but warning messages are issued wherever that analysis disagrees with the coding. This seems to me an ideal solution, and I am sure that I would not have arrived at it so readily if I had not been reading RISKS.

I now face situations in which the program has minor deficiencies that I tend to ignore. Knowing that the hand-coding is right and that it would take several hours to upgrade, I prefer to see a few warning messages flow by. It reminds me of all of the people who have ignored warning lights and buzzers to their detriment, and I am preparing to work on the program to ensure that I do not become insensitive to the warnings.

So, thank you for moderating RISKS, Peter, and thanks to all of the contributors. People occasionally complain about postings that do not deal directly and exclusively with computers; in my experience, these postings help prevent problems in software design. --Jim

James H. Coombs, Mellon Postdoctoral Fellow in English, Brown University

[Some of you look upon RISKS as a collection of anecdotes and nothing more. The old principled codger that I am, I always look for the underlying principles, which you are (sometimes subliminally) continually confronted with when you read RISKS. I think it would get tiresome to our readers if I called out the principles related related to each contribution, but you don't have to read too carefully between the lines. The "relevance" issue amuses me, because principles can be derived from or applied to cases in which the computer link is only marginal. Many of the same principles apply irrespective of the degree of computer involvement. PGN]

"Demon computer"

Peter G. Neumann <Neumann@CSL.SRI.COM>
Sun 22 Feb 87 19:01:09-PST

Once in a rare while we turn to that wonder of sources, the Weekly World News, for a different kind of news item. (An earlier one was the Chinese computer developer who was electrocuted by his old computer after he built a new one. There WWN's shtick involved his wife blaming jealousy on the part of the artificially intelligent computer that had been programmed to have human-like emotions.) The issue of 3 March 1987 had on page 3 the tale of a bank in Valpariso, Chile, that had recently installed $7.3 million worth of computer equipment, including 13 terminals. One of these terminals was used by three different people who met extreme misfortune in some strange way -- deaths of two employees and the brain-dead coma of a third. One of the deaths was attributed to a massive stroke, the other to "unknown causes". ``At first we decided to remove the terminal'', said Jorge Montalabo (VP of customer relations). ``But the workman who came to carry it away fainted when he tried to unplug it from the system.'' Since no workers will now go near the terminal, the bank is apparently going to try exorcism! ``If the exorcism doesn't work and someone else dies while using the terminal, we'll have to scrap all of our computers and spend millions getting a new system. Otherwise no one will work here.''

The issue here is of course not whether the computer terminal is possessed, but whether there could have been some harmful attribute of that particular terminal (electromagnetic or isotopic radiation, etc.). (Presumably

shutting down the entire system and removing that terminal would have made sense...) On the human side, it is not surprising that such a sequence of events would have such a profound effect on the surviving computer personnel.

It would be easy to discredit this story on the basis of other off-the-wall stories found by the WWN. Although I don't think RISKS should indulge in rampant speculation, it does seem plausible that some physical phenomenon could have been involved -- electric currents, radiation emissions, etc., and thus some open-minded curiosity about this case is in order. I wonder whether there are any RISKS readers in South America who could provide any solid information on this case! PGN

NSA Risks

Alan Wexelblat <wex@MCC.COM>
Mon, 23 Feb 87 10:21:25 CST

One thing I'm surprised no one mentioned is the RISKS being discovered at the NSA in the ongoing Iran-Contra affair. The NSA spooks (and the administration) seem to be getting burned because of *too much* backup.

For example, the false chronology of events reported by Regan and Reagan during their testimony to Congress was discovered only when someone made available the NSA's massive computer archive. Apparently every file, mail message, etc., ever created on the NSA's computers is archived there at time of deletion. It seems that most NSA people were not aware of the archive (or had forgotten about it). Messages in this archive showed how North, Casey, and Poindexter had concocted the false story.

Just recently, Oliver North's secretary turned over floppies to the Tower commission which contained undeleted copies of the memos that North et al. carefully shredded before the investigators arrived.

Results of a recent security review

Mary Holstege <HOLSTEGE@Sushi.Stanford.EDU>
Mon 23 Feb 87 10:25:19-PST

Findings of a recent security review:

The environment here is a computer software vendor, which also has a number of timesharing customers using the same computer as the programmers. Customers rely on the computer for accounting and inventory control applications.

I should first say that people at the company at which this security review took place were of the general impression that their system, and in particular directories containing their proprietary programs and sensitive customer data, were quite secure. The combination of case histories garnered from RISKS and a recently-terminated employee prompted the review,

but the general consensus before it was started was that there was no cause for concern. A couple of programmers griped about having their "time wasted" in such a "silly exercise." This turned out to have been a mistaken assumption.

Although it is unlikely that a breakin actually occurred, part of the problem with one of the security defects was that such a breakin would be untraceable. The facts are these:

The account system of this particular computer includes the ability to "share" files on other accounts. If the directory file of that account is shared one is granted access to the account as a whole. One can gain access to an account which is not shared through the use an alias command which will require a password. No such password is required to access a shared directory. Generally, aliases, failed aliases, logins, and failed logins are all logged. Secure accounts are protected by having a special "PASSWORD2" program which performs additional (user-definable) verification. This program is uninterruptible. On this particular company's system the password2 program demands that the user enter a six digit number that varies with the time of day, day of the week, and an array of random numbers presented to the user. Since the secondary password changes with each login attempt, it was felt that accounts protected in this way were immune to breakin attempts.

First problem: The proliferation of shares for the convenience of programmers. It was found that several of the programmers had permanent shares to many "secure" accounts. All the most important accounts on the system were shared with accounts that were not protected by the secondary password system. Thus, to break into one of these secure accounts one had only to break into one of the programmer accounts and alias. Many shares which had been given for some temporary project were never removed. Thus programmers who were denied knowledge of login passwords to sensitive accounts had shares to them anyway. Some *customer* accounts still had such shares left over from temporary projects.

Second problem: Poor passwords. Most of the users on the system (including the programmers) had not changed them in over a year. Most passwords were easily guessed. A programmer with shares to the most sensitive accounts on the system had a two letter password consisting of his initials. A number of customer accounts had been set up with *null* passwords which had never been changed! All this in spite of the fact that memos had been circulated advising users of the need for better passwods and relatively frequent password changes.

Third problem: Alias and login logging can be turned off on an account-by-account basis. While this does require access to the system manager's account, by (1) and (2) it was easy enough to obtain this access. What's more, at least one programmer, with shares to many sensitive accounts had turned off this logging for several accounts, for reasons which remain unclear. (Perhaps just because he was able; perhaps because at one time he had found a hole in the security system -- duly reported -- which allowed access to certain hyper-secure accounts and he had wanted to pin the hole down without having to answer a lot of embarrassing questions.) This was not discovered by the security review, incidentally, but by an attempt to

reconstruct the circumstances of a system crash.

Fourth problem: While the secondary password program is uninterruptibly run automatically with terminal logins, it is not run at all for a batch job login. Thus it is possible to break into the secure accounts by a standard password attack once one has gained access to any account on the system (although with the overhead of creating batch jobs, it's true).

Fifth problem: A program can be created with "OWNDIR" privileges. While it is running, it has all the privileges associated with the account on which it resides. So one can grant unprivileged users access to commands that require privileges by sharing such a program with them. The problem with this is that unless the program is shared execute-only instead of read-only, it can be interrupted, granting the unprivileged user access to all the privileges of the program's account. A number of such programs were shared read-only instead of execute-only. The types of privileges thus gained include the ability to bring down the system or terminate any job.

Conclusions: there were several gaping holes in the security system, and it would have been quite possible for someone to have gained access to proprietary programs or sensitive timesharing customer data without any record of the breakin being left. And all this at a company which already had in place what it considered sophisticated security policies and effective protection against breakins. One shudders to think what the situation might be at places which haven't even considered the problem.

-- Mary Holstege Holstege@SUSHI.STANFORD.EDU

[This contribution is yet another example of an old problem. Nevertheless, it is worth including. "Eternal vigilance ..." PGN]

Electronic steering

Kevin J. Belles <scubed!crash!kevinb@seismo.CSS.GOV>
Mon, 23 Feb 87 02:44:11 PST

In reply to the comment about drive-by-wire versus the F-16 fly-by-wire system, the levels of safety of the two systems aren't really comparable.

The average military aircraft gets a maintenance checkout either each or every other flight to test for system malfunction, while on an average auto you are looking at more like a checkup every 50K miles. Myself, I'd not consider purchasing a drive-by-wire auto unless it has a much better record than the computer-aided automotive systems have demonstrated so far, especially on a putative high-performance sports car model, but instead drive a car with no electronics in it to speak of (a 1966 Volvo 122S).

Although a computer enthusiast, I prefer not to bank my life on them more than absolutely necessary, knowing their ocassionally erring ways. All it would take in a system as described in previous issues would be once.

-Kevin Belles

Kevin J. Belles - UUCP: {hplabs!hp-sdd, akgua, sdcsvax, nosc}!crash!kevinb

~~ ~~~~~~ - ARPA: crash!kevinb@{nosc, ucsd}
- INET: kevinb@crash.CTS.COM - BIX: kevinb

Re: Electronic steering

Rick Sidwell <sidwell@ICSD.UCI.EDU>
Mon, 23 Feb 87 09:36:05 -0800

<> Side note: Isn't the F-16 a fly-by-wire plane? If electronic steering is
<> safe, and reliable enough for combat jets, why wouldn't it be safe enough
<> for everyday car?

Combat (and other jets) are maintained much better than cars, in general. The FAA requires every airplane to pass a pre-flight check before the first flight of each day. How often does the average person give a pre-drive check to his/her automobile before driving to work?

I was once driving a car when it suffered a complete power failure. The main cable from the battery had somehow worked it way next to the engine (probably during a battery replacement), and the heat melted through the insulation, shorting the +12 volt line to ground. Everything stopped: the engine, the radio, the clock, etc. Fortunately, the power steering and power brakes worked even without power, and no damage occured. I hate to think what would have happened if the car had had electronic steering.

I am not against electronic steering in principle; it does have its advantages (if they design it right, it should be much easier to perform such maneuvers as parallel parking in tight spots and making U-turns on small streets). But I would hope that the designers take into consideration the possibility of a sudden and complete power loss while driving.

Re: electronic steering

Kevin Oliveau <oliveau@think.com>
Mon, 23 Feb 87 12:21:20 EST

One RISKS reader (RISKS-4.49) asks why a system that is safe and reliable enough for combat aircraft would not be safe enough for a car?

The answer is that combat aircraft receive a great deal of care and preventive maintenance. Cars, on the other hand, are often driven without being properly maintained and their systems are not repaired until they break down. Mechanical systems are fairly reliable and degrade faily smoothly. (Brakes often make noise or become "mushy" before failing completely.) Electronic systems tend to simply stop working. So in today's car, you drive through a puddle and your engine dies (perhaps the power steering dies as well), but you will have control of the car: you can steer and brake. In tomorrow's car, you'll drive into the oncoming lane without any control at all.

Kevin Oliveau

[Electronic systems need not just stop working -- they may have failure modes that bear little resemblance to physical principles. A wild transfer in a program or a dropped bit may result in strange behavior.

Wet brakes may fail in either case. For that matter, in each case there is the possibility of overreaction. (I am reminded of the 1950's tale about the Swarthmore students who greased up a train track approaching a station. The engineer applied full brakes when the train did not slow down; at the end of the greased section, the train and the clean track did not react well to one another...) PGN]

Re: electronic steering

<markl@JHEREG.LCS.MIT.EDU>
Mon, 23 Feb 87 17:01:19 est

>Side note: Isn't the F-16 a fly-by-wire plane? If electronic steering is
>safe, and reliable enough for combat jets, why wouldn't it be safe enough
>for everyday car?

(The following may be apocryphal...) A friend of mine once told me that the first time a prototype F16 was taken out on the runway, its test pilot tried to retract the F16's landing gear while on the ground. The gear happily did so. This caused a fair amount of damage to the F16. My friend speculated that this might not have happened had the F16 not had a computer between the pilot and the landing gear. I'm not at all convinced that remote steering and such-like are safe at all. I can just see the folks at GM forgetting a couple of lines of code in some important part of the steering program...

And there is another problem which I am not sure has even been brought up here. Aircraft are supposedly meticulously maintained (unless they are owned by Eastern...). Even with this high quality maintenance, accidents happen. What do you suppose will happen when you put sophisticated computer steering equipment in a car that gets serviced when the owner feels like it? We have enough trouble forcing cars to pass safety and emissions control inspections without having to depend on car owners to get their on-board steering computer inspected every year.

Mark L. Lambert

MIT Laboratory for Computer Science, Distributed Systems Group
Internet: markl@jhereg.lcs.mit.edu

[Yes, I noted the overlap in the last four messages. But each made a different point, so I did not reject any... PGN]

Report problems with the web pages to the maintainer

Search RISKS using swish-e

THE RISKS DIGEST

Forum on Risks to the Public in Computers and Related Systems

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

Volume 4: Issue 51

Tuesday, 24 February 1987

Contents

HiTech version of NixonTapes

Pete Lee <lee%cheviot.newcastle.ac.uk@Cs.Ucl.AC.UK>
Tue, 24 Feb 87 15:17:19 GMT

This originated in New England, not Old England ... and is from the Boston Sunday Globe, 22 February 1987, editorial page.

WHAT THE COMPUTER KNEW

The Reagan presidency may become the first to be done in by a computer. While legislators, investigators and reporters go sniffing down the money trail, trying to track the flow of funds from Tehran to Geneva to Honduras, an electronic archive in the White House has been leaking the most embarrassing facts to the Tower Commission.

It is an irony of the computer age that an administration obsessed with secrecy allowed many of its secrets to be saved in an

electronic memory bank. All the computer messages Oliver North and his collaborators in covert action sent each other since Nov. 8 have been preserved.

A nonpartisan system of software is now telling the Tower commission not only about the hardware sent to Ayatollah Khomeini, but also abut frantic White House efforts to save the president from scandal. The backup system for the White House computer reportedly shows that the president's men tried to alter the history of what they did in order to distance Reagan from his ill-considered policies.

The computer messages are being compared to the tape recordings of Richard Nixon. If they demonstrate a White House attempt to design a cover-up, they may play the role of the Nixon tapes in the Watergate scandal.

Messages indicating that North passed military intelligence to Tehran, for use in Khomeini's destabilizing war against Iraq, suggest that even now the White House has not told the full story of Reagan's concessions to the ayatollah.

By preserving the tamper-proof truth of what government officials did or did not do, the electronic archive in the White House may add an unforeseen dimension to the system of checks and balances bequeathed by the Founding Fathers.

This computer was not user-friendly.

[Several readers noted that Alan Wexelblat meant NSC and not NSA in his message in RISKS-4.50. However, I recall that several key NSC phone conversations had been monitored by NSA fairly early in the game.

The NSC archives remaining even after on-line copies were deleted and hard-copies shredded is of course another instance of the hidden-residue problem in (allegedly) secure systems, i.e., a deletion is a deletion is not a deletion! By the way, the assumption that the archives are tamperproof is of course bogus. PGN]

Re: Automatic Call Tracing for Emergency Services (RISKS-4.49)

Lee Naish <munnari!mulga.OZ!lee@seismo.CSS.GOV>
Tue, 24 Feb 87 16:11:09 EST

I once spoke to someone who helped set up the fire brigade database in Melbourne. The system they use is to specify the intersection of two streets. Initially there were various integrity constraints in the database, such as street names had to be at least two characters long, streets didnt cross each other more than once etc. Two streets violated both conditions: S street (shaped like an S) crossed another street in three places and Y street (shaped like a Y) crossed another stree in two points (numbering must be rather confusing in Y St.!). (The real world is not designed for computers; pity :-)

lee

Air Traffic Control, Auto-Land

<mmachlis@ATHENA.MIT.EDU>
Tue, 24 Feb 87 11:37:44 EST

Is there anyone on this list who knows whether the air traffic control radar systems have automatic collision alert systems? And if they do, do they work? It seemed to me that if everyone were required to have Mode C transponders (which automatically report the plane's altitude to the nearest 100 feet to the ATC computer), then it would be simple to write a program which would detect possible collisions. Arguments against this may include that the controller would have much too many targets on his screen to handle -- as it is now they often screen out all traffic that they are not working with so that the planes do not even appear on their radarscope. However, a program such as I suggested could work on all planes, whether actually being displayed on the scope or not, and maybe bring to the controller's attention two planes on a collision course and altitude which were not being displayed and would not have been noticed.

[It is my understanding that the ground-based AUTOMATED collision alerts will be a part of the new system (currently in procurement). But the expense of the on-board equipment seems to mitigate against its use in small private planes, which preset a very serious gap in the on-line information. 3-D radar might be more appropriate, especially since a Mode-C transponder could be faulty... PGN]

Another thing: what are people's opinions about autoland[ing]? This system, installed on many of the large passenger jets, will take over control of eveything -- rudder, ailerons, and throttles -- from up to 20 miles out from the airplane, fly the approach, flare the plane, and actually touch down, all automatically. At present I believe only several thousand complete autoland cycles have been flown at all. I read in an aviation magazine an article written by a 30,000 hour airline pilot about it; he said when he went along for a demonstration of autoland it flew a flawless approach, and he rated it well above the average human approach. Plus it can do this is any weather at all (in terms of visibility and cloud layers). Certainly computers are not infallible, but neither are humans. It may be true that if pilots always used autoland they would not retain the flying skills to take over in case of failure, but in some cases I can certainly see a use. For instance, a common time for minor incidents is when a plane is nearing its destination after a long international flight. After the crew has spent maybe 4 hours acting only as "system monitors," now they must suddenly start talking to people and actually flying the plane. If one would say that autoland is not good because pilots' skills would deteriorate, is this not true of the autopilot, which does the flying for a large part of most flights?

-Matthew Machlis

[For the AI community, I could not resist pointing out that whether or not this message got included might be determined

by a variable "MachlisP". PGN]

Electronic steering

Spencer W. Thomas <thomas%utah-gr@utah-cs.arpa>
Tue, 24 Feb 87 17:22:34 MST

Seems to me a point that the other respondents missed here is that in a military system, people are prepared to accept a certain number of deaths due to failure, in order to have a higher performance system. Look at the number of military planes that crash while on maneuvers, and no-one thinks much about it. Similarly, one might put electronic steering on a race car, if it was felt to offer a competitive advantage, and if the car crashed during the race, "them's the breaks".

=Spencer ({ihnp4,decvax}!utah-cs!thomas, thomas@cs.utah.edu)

[Another message on this subject was received from William Swan: ... Military planes undergo a lot of maintenance, logging, as I understand it, as much or more service time than flight time (if I am wrong, please provide the real numbers). ...]

Hurricane Iwa and the Hawaii blackout of 1984

Matthew P Wiener <weemba@brahms.Berkeley.EDU>
Tue, 24 Feb 87 01:48:18 PST

[With respect to the WWN computer terminal story:]
You might wish to read Stephen King's short story "Word Processor of the Gods" in his collection _Skeleton Crew_.
ucbvax!brahms!weemba Matthew P Wiener/UCB Math Dept/Berkeley CA 94720

From: bob@uhmanoa.UUCP (Bob Cunningham)
Newsgroups: sci.misc
Subject: Re: James Burke (what a real blackout is like)
Date: 17 Feb 87 17:57:55 GMT
Organization: Hawaii Institute of Geophysics

On Thanksgiving evening 1984, Hurricane Iwa---essentially without warning---hit the islands of Kauai and Oahu, destroying major portions of the electrical grids on both islands and knocking out all electrical generation. It was several days before power was restored to portions of Honolulu (incidentally, the 11th most populous city in the United States), several weeks before power was completely restored. One of the reasons it took so long was that all of the generators were designed to be "jump-started" from another running generator on the grid, and no one knew how to bootstrap up a generator all by itself.

The whole story is rather too long to go into here, but here are some of the key points...

There was no satellite meteorological coverage for the central Pacific, because the GOES East satellite had failed, and the GOES West had been moved over to cover the Atlantic...which the Weather Service figured was more important. Weather observations from ships told of a strong hurricane developing west of the islands, but a military reconnaisance flight sent out on Thanksgiving day failed to accurately locate the storm. There was no historical precedence for the path it took that led right to the population centers.

In the afternoon, winds started rising, and the Weather Service issued a Hurricane Watch, then quickly a Warning, but still didn't have a precise fix on Iwa, nor accurate information on speed or direction.

Early in the evening, after dark the winds started gusting well above 60 mph, and the electrical grid went down, surprising the electrical utilities who had taken no precautions to isolate any of their systems...taking down all their generators.

[This could be a separate story in itself, but suffice it to say that the Civil Defense Emergency Broadcast system didn't work. Besides all the TV stations, all the radio stations---except one--- went off the air that night. The single radio station that had an operating emergency generator was running "on automatic", playing religious music.]

By the next day, one or two other radio stations were up (and the religious station had hastily converted to all-news), but power was still out... remaining out for days. The first thing people missed was water, the water distribution system being driven by electrical pumps...though some places that had gravity feed from tanks above in the hills were lucky for a while.

Traffic was a shambles since no traffic lights were working... though that became less of a problem over the next day or so since no gas stations were pumping and people realized that they were stuck with just whatever gasoline they happened to have in the tanks of their cars, and started being very careful about how they used that up.

Food in refrigerators and freezers spoiled. Long lines developed at grocery stores as people tried to buy more food...and clerks had to add up by hand. Most resturants stayed closed; the few that opened---cooking with gas---soon closed again as the city gas system began losing pressure.

Electrical generators (even small ones) were not available for love nor money, ice and candles (when available) went for premium prices.

The most-listened-to person in the islands was the spokesman for the electrical company who spent virtually all of his waking hours on one radio station or another detailing the repair work underway.

Meanwhile, the electrical utility company crews worked around the clock to restore portions of the electrical grid, and devise ways to start up even one major generator. I don't know the full story behind the restart effort, except that lots of different techniques were tried, one of which finally worked on Oahu. The Navy dispatched a nuclear submarine to Kauai in an effort to "jump start" the main generator there.

It seemed like forever, but it was only a few days until electricity was available to some parts of Honolulu.

We lived with rolling blackouts for about a week more. Outlying areas on the islands weren't fully restored for over two weeks.

There were some fatalities, due mostly to "freak" accidents of various kinds...and a small, but statistically significant "baby boomlet" some 9 months later. If this had happenedd to a major mainland city in winter there would have been considerably more fatalities, and the story would be much more widely known. As it was, if it had lasted too many more days, water would have become very critical...

Bob Cunningham bob@hig.hawaii.edu

Summary of a Talk by SANFORD (SANDY) SHERIZEN on Computer Crime

Eugene Miya N. <eugene@ames-pioneer.arpa>
24 Feb 1987 1812-PST (Tuesday)

FUTURE TRENDS IN COMPUTER CRIME: THE POST-HACKER ERA

Dr. Sandy Sherizen is a criminologist and former information security expert who consults with corporations, banks, and Government Agencies on the prevention of computer crime. Dr. Sherizen began his discussion by giving an impression based on the development of safes and safe cracking. He talked about the overly technological nature by which safes improved and safecrackers got better.

What is important about Sandy speaking is that criminology is a well-founded science and that many of the patterns in computer security have been studied already in criminology. (Sandy finds this shocking.) We would do well to learn from it.

Let me try to reproduce the sequence. First, safe were created, and crackers broke the locks. Locks got tougher. They went to combination locks (and lock picking, separate area). Next, they resorted to drills, and the countermeasure was stronger metal. Next came simple explosives again followed by heftier metal, and more powerful explosives. Around this time, they discovered nitroglycerin which as a liquid can be poured into cracks. They then discovered the use of oxyacetylene torches to cut thru. Safe makers retaliated with heat-conducting materials. During this time, people started kidnapping bankers and their families (a totally non-technical solution to the problem). This problem was "solved" using time-locks on doors. (I enjoyed the last example.) Crime goes on.

In Sandy's thesis, there are 4 stages that we have to deal with in terms of computers, and the talk itself was a series of rambling discussions. The 4 stages, by the way, which worked in the case of banks, safes, and vaults, are detailed in a book in Criminology which we can get as a reference.

Sandy's concerns are first:
privacy, work, monitoring of work
computerization of crime
information property

Sandy also made some interesting comments, for instance, on the development of laws -- the concept of "moral entrepeneurship", a very different kind of thing than most computer people are used to.

The Tylenol drug poisoning case is an interesting case -- the point is that no new laws were created, but a technological solution of tamper proof packages came into use. That corporation on the whole had no policy for dealing with problems of this kind to begin with, and had inadequate protection in understanding them.

The reasons for commiting crime are interesting Criminological and Sociological areas. Basically, the common threat is a "trusted embezzler" with an "unsharable resource" or "unsharable problem", and there are what is called the 3 B's starting with Booze as the reason why people do regular crimes. The reason why people commit computer crimes is what is called the 3 C's:
cash
career
challenge

Sandy also mentioned the fact that the media basically regards computer crimes as hi-tech soap opera. We make criminals folk heroes, but at the same time we have to be able to protect whistle blowers.

The 4 stages in EDP growth have similar trends or patterns in the nature of computer crime. This is called the Gibson-Noland Law on EDP growth. The 4 stages:
initiation
expansion
formalization
maturity
as generalized to computer crime initiation begins with
first hit or miss crime
such as in Steven Levy's book, "Hackers" which is popular and we are transitioning out of this phase into a phase of
expansion
which includes lots of people and undetectable crime with many rewards. [We are] beginning "specialization," which is a formalization stage of crime where the law gets into the act and the criminals themselves specialize in criminal things like financial systems, or UNIX Systems, and so forth, but in the formalization stages law gets interested and finally the fourth stage of maturity there are a relatively predictable sequence of crimes. Such as, there is measure and countermeasure on part of the law enforcement as well as the criminals themselves.

Sandy's basis for this talk is that were going to see new types of crime with a new series of targets: a new sense of how-to-do crime and how-to prevent crime. Basically, they are categorized by the 414's (the Milwaukee WI area code), teenagers who broke into computers.

When asked by a Congressional committee when he realized that he had done something wrong, Neil Patrick pointed out "When the FBI was knocking on my door" -- there basically was hunt and peck computer crime.

So Sandy's predictions for future directions of computer crimes are threefold:

> First of all there will be fewer crimes on computers, but they will be of a much more serious nature, because there is survival of the fittest -- and organized crime will get into it. We see some people who won't quit but who have to learn about criminal elements such as, laundering money, not leaving fingerprints, and so forth which would basically defeat the older generation criminals.
>
> The second thing will be more technological opportunities to commit crime, such as photocopying with copying machines and money.
>
> The third prediction is more internationalization of crime. (There was a brief aside after the internationalization regarding viruses, and the typical example of this was given in the piece of software known as eggbeater and also by the book Soft War -- eggbeater was a program that literally ate up data and dropped away ...)

Another area of concern was the area of modes of learning about crime. Sandy was concerned with the suicide epidemic noted by the Center for Disease Control, and uses the name "copy-cat crime". (Example of copycat crimes are in the movie "War Games" and in use of Automatic Teller Machines (ATM).)

The professionalization of crimes involves such things as raids and reverse-engineering files and records not just in a sense of building things. But changing records -- we're going to see more. Again, the evolution of specialization -- more collusion perhaps between individuals who commit crimes. A good example of this is the Walker spy trial; this is a serious crime but the public will not see it as a serious crime, just as it does not see white collar as a serious crime.

Part of the problem is that we look upon things such as pens and pencils as free, which come with the territory as far as working. Because of offices, nobody thinks of it as a crime unless you come literally and haul the pens and pads away using a truck; that's just like taking a disk for a computer home, its not really regarded as a serious thing unless the entire payroll is located on it. So a large part of this is public awareness and education in terms of how to deal with crime.

Privacy is the issue that we really probably need to work on the most, Sandy said -- the needs and problems of technology invading privacy and that what we should do (in particular) is worry about that as opposed to trying to solve all computer crime problems.

Sandy is a friend of Dr. Lucy Suchman at the Xerox, Palo Alto Research Center (PARC) and if we want to get in any further contact with him the best thing to do is contact him through Lucy. I believe he's

teaching at MIT. Also in attendance was Donn Parker (SRI International) who is also well known.

There was considerably more discussion than was involved on this tape. Correspondents should send electronic mail to me, for further information.

[Lightly edited. Garbles could be mine or Eugene's ...
This is included primarily for our newer readers, in that RISKS has gone over much of this ground on various occasions in the past. PGN]

Search RISKS using swish-e

THE RISKS DIGEST

Forum on Risks to the Public in Computers and Related Systems

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

Volume 4: Issue 52

Thursday, 26 February 1987

Contents

B-1 plagued by problems

Peter G. Neumann <Neumann@CSL.SRI.COM>

Thu 26 Feb 87 21:12:09-PST

(From the Stanford Daily, 26 Feb 87, in the "Dateline" section, compiled from the wires of the AP and the LA Times/Washington Post News Service)

WASHINGTON -- Government investigators said Wednesday that as many as half of the new B-1 bombers at a Texas air base have been grounded in recent weeks because of nagging technical problems and that the aircraft's shortcomings may persist well into the next decade, contrary to public statements by the Air Force. During hearings before subcommittees of the House Armed Services Committee, Chairman Les Aspin, D-Wis, said the bomber's heart -- its defensive electronics system -- not only fails to jam enemy radar signals but actually serves as a beacon illuminating the B-1 as a target. Government Accounting Office officials ... testified that the problems with the $28.3 billion bomber program, especially the critical defensive electronic countermeasures (ECM), are far more serious than Air Force officials have acknowledged. GAO officials also predicted that the Air Force will have to ask Congress for substantially more money in coming years to repair and upgrade the bomber.

Computer loses bus

Mark Biggar <markb%sdcrdcf.UUCP@JOVE.CAM.UNISYS.COM>
Thu, 26 Feb 87 10:58:17 pst

The Los Angeles bus system (also known as the Rapid Transit District (RTD)) uses a computer to keep track of its buses. The computer knows which bus is traveling which route at what starting time. The computer also has the complete time schedule information. The computer can be used to estimate the position of any bus using this information.

On Feb. 25 the driver in trouble radio alarm was set off on bus #181, the computer was asked where the bus was and the LAPD was notified. The LAPD patrol unit that responded to the call could not find the bus, so they called in more units. They still could not find the bus and asked for a helicopter to help search for it.

After about a hour, the bus driver was located in the drivers' lounge at the bus yard. The bus was in the repair yard and the repair crew had accidentally set of the alarm. It turned out that the driver had assumed that the repair yard had told the RTD computer that the bus was out of service, and the repair yard thought that the driver had told it.

Mark Biggar Unisys - System Development Group, Santa Monica
{allegra,burdvax,cbosgd,hplabs,ihnp4,akgua,sdcsvax}!sdcrdcf!markb
markb%sdcrdcf@CAM.UNISYS.COM

Human errors

Brian Randell <brian%kelpie.newcastle.ac.uk@Cs.Ucl.AC.UK>
Thu, 26 Feb 87 19:11:49 gmt

There was a very interesting documentary on BBC TV in their QED series here last night, entitled "A Fall from Grace: Patterns of Human Error", which contained quite a bit of material of relevance to RISKS.

The programme (Yes, that is how even I spell it when it isn't intended for a computer!) used as its principal illustrations the 1977 collision of two Jumbo jets at Tenerife airport, and the task on making tea! Various types of human error were described, and discussed with several experts, including Professor Jim Reason, (Dept of Psychology, Univ. of Manchester), Dr. Ivan Brown (Applied Psychology unit, Medical Research Council), and David Embrie (sp?), an ergonomist from Aston University.

The principal thing which I learnt, to my shame, from the programme was that psychologists seem have done a lot of useful study of the many different types of errors that even highly trained human beings make when exercising a sophisticated skill.

Some comments I jotted down:

(1) One could learn much of relevance regarding the errors made in carrying out highly skilled safety-critical tasks, such as piloting an airplane, or in a nuclear control room, from studying the errors made in inconsequential tasks (hence the tea making example, which when you think about it, does involve considerable, albeit informal, training) - i.e., the underlying causes seem to be similar, even if the consequences of errors are grossly different.

(2) With a highly skilled activity, you make more mistakes if you do it consciously. This particularly applied to "sequencing" errors, such as missing or repeating a step. For example, if you are so following a well-known sequence of actions, on mental auto-pilot, and then suddenly become aware of your actions, there is a good chance of your resuming the sequence at the wrong place.

(3) When you have learnt two similar sequences, you have, so to speak, constructed two similar competing "action daemons" - one can acccidentally switch to the wrong one. This was illustrated with an account of how one of the pilots (who was very skilled, and spent much time training others) was thought to have reverted to a pattern of actions which he was familiar with from simulator training, which did not quite match reality in the way that the pilot was supposed to communicate with the air traffic controller.

(4) One characteristic of error-proneness concerns the notion of "field dependence" - some people have difficulty, and are slow, at picking out a relevant object from a complex field of view - a sort of mental tunnel vision, for which there are standard tests. Pilot training would probably select such people out, but drivers might well suffer from this, and the idea of using the standard tests to decide whether someone should have a driving licence was unlikely to be acceptable.

The programme also contained a well-illustrated, though to me rather more expectable, account of the problems of designing interfaces to try to minimise human error - mainly illustrated by control room design, with reference to

Three mile Island.

Today I telephoned Prof Reason, and had a very interesting chat with him. We have arranged that he will come and give a talk to our Systems Research Group, and I have been given the following interesting sounding reference: New Technology and Human Error (ed. J. Rasmussen, K. Duncan, & J. Leplat), Wiley 1983, to which he contributed several chapters. My hope is that his ideas on error classification might be of relevance to the sorts of problems that s/w (and h/w) engineers suffer from which result in residual design errors in complex computer systems.

My apologies to readers for whom all this is familiar - perhaps I should have taken Psychology 1, after all!

Brian Randell - Computing Laboratory, University of Newcastle upon Tyne

ARPA : brian%cheviot.newcastle.ac.uk@cs.ucl.ac.uk
UUCP : <UK>!ukc!cheviot!brian
JANET : brian@uk.ac.newcastle.cheviot

Possessed terminal?

<pom%under.s1.gov@mordor.s1.gov>
Thu, 26 Feb 87 09:48:41 PST

Since WWN is usually quite authentic, I will entertain some speculation on the topic. While 'electric currents' cannot be ruled out (an incompetent electrician could put full voltage into the 'ground' and many countries use 220V rather then US style 110V), the most likely explanation seems be the good old 'VDT stress'. (VDT = Video Display Terminal).

There is a big volume of writing on the topic and even some solid information. Radiation (soft x-rays from CRT) was often blamed but informed consensus (which agrees well with my own observations) is that stress is psychological. Introduction of any 'computerised system' could be an enormous trauma to people who were never exposed to the computers (even when all you do is replace IBM Selectrics with the word processors <=:: I have seen secretaries crying and thinking of quitting or even retiring from the workforce for good).

The proper procedure for converting to computer system is as follow:

1) Introduce terminals to the workplace, while doing the 'real work' with the old, manual system.
2) Put some games on the machine and let people play with VDTs (perhaps after hours or during lunch breaks).
3) Introduce e-mail, first just as alternative to phone call or memo, so that it is not NEEDED to get the job done.
4) When everybody (as measured by volume of use) is comfortable with the system, put some work-functions on the new system.
5) After a month or two, convert the rest. (You may find out that some people will quit or ask for a transfer, even with slow transition;

those requests for transfer should be honored from the start.)

I wonder how may 'mysterious accidents' that occur after new 'sophisticated safety systems' (e.g. in nuclear power plants) are introduced are caused by ignoring these simple common sense rules.

pom

Entertainment risks

<thode@nprdc.arpa>
26 February 1987 0736-PST (Thursday)

I generally favor the broad interpretation of what gets into this list. In that spirit, I offer the following item from the San Diego Evening Tribune of Feb. 25. It may or may not be "computer risk" related:

"Los Angeles (AP) - Dialing a telephone is sometimes a gamble, as callers found out when they got "Dial-Porn" instead of state lottery information because of a switched line.

"Pacific Bell fixed the problem yesterday, but before that callers heard a suggestive recorded message from a sultry-voiced woman when they sought Saturday's winning lottery numbers.

"Maria de Marco, who manages 976 prefix lines for Pacific Bell, said it wasn't known whether the switch was a prank or an accident..."

[Since most telephone systems are now extensively computer controlled, this certainly falls into the class of human misuse of computers. PGN]

In the same paper there was another item, also datelined Los Angeles, that described the confusion of some Lawrence Welk compact disk buyers when their mislabeled and mispackaged CDs turned out to contain the soundtrack from a movie about former Sex Pistols member Sid Vicious.

[I decided not to delete this paragraph on technology-irrelevance grounds. It could have been a computer-related problem! PGN]

If a computer is involved in these instances, it would appear to be one with a sense of humor.

--Walt Thode (thode@NPRDC)

[Even if one wasn't involved, it has a sense of humor! PGN]

Re: Automatic Call Tracing for Emergency Services

James Roche <roche@rochester.arpa>
Wed, 25 Feb 87 10:29:45 est

[...]
As a firefighter in Monroe County (where Rochester is located) I can offer some insight to the troubles of the 911 system here. The 911 dispatch center here provides services for more than 80 county-wide emergency agencies (police,

fire, ambulance). That is reportedly more than any 911 center in the US.
Among the problems encountered are that fire district boundaries don't match
postal service boundries which don't match ambulance service boundries which
don't match town boundries, etc. Therefore when the ALI indicates a particular
address is in Town X is is necessary for the dispatcher to turn to another
screen and determine which police/fire/ambulance agencies are to be dispatched.

Other problems encountered with 911 include the fact that the entire county
is served by more that one phone company. Most of the county is served
by Rochester Telephone which has set up its computers to route all
Monroe County 911 calls to the 911 dispatch center. There are however
locations in the county which are served by New York Telephone. NYT has
set up its computers to route the 911 calls from Monroe County to the
Syracuse dispatch center (70 miles east). The dispatcher on the Syracuse
end must recognize the call is from Monroe County and route the call to
the Monroe 911 center. There are also areas of the county served by
Ogden Telephone. I don't know how they handle the 911 calls.

> >(Incidentally, the county Commissioner of Public Safety took this
> >occasion to complain about duplicate street names within the county ...

While it is not clear that eliminating duplicate street names would
have avoided the above problem, it would eliminate other problems.
Not all emergency calls received by the 911 dispatch center come in
via the 911 number. Many calls are still received on the old 7 digit
number. When a call comes in on that number the pertinent data for
the address is not displayed. The dispatcher must then determine
which one of the many duplicates the caller is referring to. I recall hearing
6 fire departments dispatched one day to a false alarm on East Avenue
because there are multiple East Avenues within the county. The call
was received on the 7 digit number and the caller gave incomplete
information to the dispatcher (intentionally I imagine). The county feels
that it must continue to provide service on the 7 digit number since
for many years phone stickers were distributed with that 7 digit number. Also
the residents the the areas served by New York Tel are encouraged to use
the 7 digit number to avoid delays by going through Syracuse.

Jim Roche UUCP: rochester!roche
University of Rochester Computer Science Department Rochester, NY 14627

Re: Automatic Call Tracing and Addresses

Charley Wingate <mangoe@mimsy.umd.edu>
Thu, 26 Feb 87 23:44:03 EST

Here in Howard Co. Md., the county government took a big step years ago and
renumbered all the addresses so that with in some quanta the street numbers
are not only unique, but they also give the physical location of the property.
This has done wonders for getting the FD to the right place. Unfortunately...

"Laurel" phone exchanges lie in four counties; Laurel zip codes in three.
This makes dialing 911 a bit of an adventure because you had better know

which county you are in. Sometimes even this doesn't help. One zip code was believed by the counties to lie entirely in P.G. county, when in fact a small piece of it lay in Montgomery County. This meant that these people got no county services-- no fire, no trash, nothing. After years of bickering, the Postal Service cut the gordian knot and created a new zip code just for these people. The moral: "Garbage in, Gospel out" doesn't just apply to computers; they can "bless" information that never came near them!

C. G. Wingate U of Maryland, Dept. of Computer Science, Coll. Pk., MD 20742

"Active" car suspensions

Graeme Dixon <graeme%cheviot.newcastle.ac.uk@Cs.Ucl.AC.UK>
Wed, 25 Feb 87 19:14:57 GMT

Since the discussion has once again come around to the use of computers in cars the "... most important single automotive advance since the accelerator pedal ..." may be of interest.

There have been a number of articles in British motoring magazines (Car Oct 86, Fast Lane Jan 87) over the last few months describing the Lotus "Active" suspension. This consists of a replacement for the normal passive suspension of dampers, springs, and anti-roll bar, by a sensing system, computer, and a set of hydraulically controlled actuators. The sensors return the cars relative movement and driver inputs, and the computer adjusts the actuators to compensate. The resulting handling characteristics are by all accounts superb - no roll, no understeer, no oversteer, just perfectly balance handling. Various parameters used by the computer may be adjusted to provide different levels of ride, prompting one of the writers to speculate that it would "be possible to build a schizophrenic car with His and Hers alternative handling at the flick of a dashboard switch."

One of the more contentious claims of the system is that "it is truly fail-safe". By providing a "get-you-home stand-by suspension" computer failure does not render the car unusable. One of the articles even describes the cars behaviour when the system is "dumped" as the car is negotiating a corner - the car switches suddenly from neutral handling to oversteer prompting the driver to think one of the rear tyres had punctured. What they didn't try was the effects of over compensation though!

It will be a few years before active suspensions appear in cars (Lotus are intending to use it in their supercar the Etna which they are currently developing), but given that Lotus have been recently bought by GM, and a number of rivals (notably Mercedes-Benz) are developing similar systems, then this should provide another fertile area for discussion when the time comes....

Graeme Dixon

Altitude-Detecting Radar

<mmachlis@ATHENA.MIT.EDU>
Wed, 25 Feb 87 16:10:34 EST

It is true that Mode C capability costs a bit of money, but I think the majority of people who own planes could afford the extra $1500 or so, especially considering the added safety.

As to 3-D radar, it would be very nice but I am under the impression that it is quite impossible, realistically speaking, with the present technology. A professor here at MIT who flew for the Navy for 20 years told me it is reasonable to make altitude-detecting RADAR, but that it is only economically reasonable for tracking a single target at a time. Aircraft such as the F-14 and F-16 can track several targets at once, but those systems are very expensive and have MTBF averages of only several hours of operation because of their complexity.

Re: Results of a recent security review

Andrew Klossner <andrew%hammer.tek.com@RELAY.CS.NET>
Wed, 25 Feb 87 12:59:02 PST

> "Fifth problem: A program can be created with "OWNDIR" privileges. While it is running, it has all the privileges associated with the account on which it resides."

Interesting ... did they license the use of this invention from AT&T, the patent holder?

-=- Andrew Klossner (decvax!tektronix!tekecs!andrew) [UUCP]
(tekecs!andrew.tektronix@csnet-relay) [ARPA]
Tektronix, Inc., Wilsonville, OR

> [... and will someone sue AT&T if, after a license is duly obtained, a devastating Trojan horse is perpetrated using this flaw/feature ? PGN]

Re: Sherizen talk; auto-landing

Eugene Miya <eugene@ames-nas.arpa>
Thu, 26 Feb 87 16:23:03 PST

I think an apology is in order. I sent my notes to the CPSR Sherizen talk to Peter (not with the intention of posting to the net). Locally, we are trying to have discussions on security trying to forego problems of discussing security both when it was tried in unix-wizards (and it subsequent list) and info-vax (for the VMS side). Although the Sherizen meeting of CPSR was open, our other meetings are not (they are not classified either).

Regarding auto-land: I don't know if I would trust such a system yet. I know few pilots who would not feel at least a little uncomfortable. Actually, I think systems like this would be great Darwinian tests of

AI. The posting implied we control everything. This is not true.
The plane is not everything, there are other planes and obstacles out there.

Put the developer on the plane, let his or her system land the plane.
If the plane survives, the developer goes on to create their next system.
(Might not be enough, but a good first cut.)
Similar tests for things like MYCIN, etc. can be used (infect using a blood disease, developer then must trust system for diagnosis ;-). Sound a little too real world? We know less about the real world than many think. Thinking is not enough.

--eugene miya

[In the past I have been extraordinarily careful about not including obviously personal messages without explicit permission. In this case I clearly goofed. The message somehow seemed to be of general interest and addressed to a large list... And it was getting late. Sorry, Eugene... PGN]

Air Traffic Control, Auto-Land

Scott E. Preece <preece%mycroft@gswd-vms.ARPA>
Wed, 25 Feb 87 09:13:49 CST

Use of automated landing also would leave the crew more free to spend its time looking for things out of the ordinary -- unreported traffic, patterns of air movement, the effect of the wind on preceding traffic, the overall condition of the aircraft -- that automated systems are not good at detecting.

scott preece, gould/csd - urbana, uucp: ihnp4!uiucdcs!ccvaxa!preece

Risks of autopilots (and risks of solutions)

Bill Janssen <janssen@MCC.COM>
Wed, 25 Feb 87 17:02:01 CST

In Risks Digest 4.51, Matthew Machlis questions whether there may be risks of pilots losing their flying skills, due to flying for extended periods on autopilot.

At a conference last year, I spoke to folks from a major commercial aircraft manufacturer, who were concerned about the same thing. (One of the speculations about KAL 007 was that the pilots just `lost track' of what they were doing.) This firm had the thought of dividing the cockpit in two, using one half for flying the real airplane, and the other half for a training simulator. The pilots would trade off acting as `system monitor' and practicing `real' problem flying. The problem with this solution was loss of orientation, along the lines of "Oh, damn, I just put the plane in an unrecoverable spin; well, restart... that's funny, nothing seems to happen... Ohmygod, I'm sitting on the *real* side".

Bill

Another difference between electronic control in cars and fighters

Brent Chapman <chapman%mica.Berkeley.EDU@BERKELEY.EDU>
Thu, 26 Feb 87 17:03:14 PST

Another key difference, which to me seems just as important as the maintenance issues already mentioned, is that cars (generally!) aren't fitted with ejection seats. A driver can't punch out when things get weird.

Also, cars tend to be operated in much more crowded conditions. Usually in fighters (except possibly during takeoff and landing), you really don't have to worry about what your plane will come crashing down on, because most operations (both real and training) occur over very sparse areas. In a runaway car, on the other hand, you stand a significant chance of wreaking considerable havoc among other vehicles travelling in your vicinity, as well as bystanders and property near the roadway.

Brent

Re: Hurricane Iwa (RISKS DIGEST 4.51)

Scott Dorsey <kludge%gitpyr%gatech.csnet@RELAY.CS.NET>
Thu, 26 Feb 87 12:24:31 est

Winds from Hurricane Iwa passed through a small mountain pass, gathered pressure from the narrow slit, and knocked out power lines which carried power to most of Central Oahu. They also did serious damage to an army base on the exiting winds side of the pass, opening warehouses filled with emergency supplies like sardine cans, or ripping the prefabricated buildings away from their foundations while leaving the contents sitting.

The base was without power for three weeks, and without water for about two. The Mayor of Honolulu asked the military for help, and they refused (being much harder hit than the civilian community, mainly due to the damage at this base). There were several scathing editorials in the Advertiser, but the military did not really release any information about the extent of the damage.

The island of Kauai was worst hit. Although the generating system was not heavily damaged, there was no way to restart the generators without power, as no one had foreseen that all the turbines would go down at once. The Navy sent a nuclear submarine from Pearl Harbor over to Kauai to provide power for the starters, but by the time it arrived, the engineers had restarted the system, using almost a hundred automotive batteries.

> In the afternoon, winds started rising, and the Weather Service issued a
> Hurricane Watch, then quickly a Warning, but still didn't have a precise fix
> on Iwa, nor accurate information on speed or direction.

At about noon, state employees were sent home, schools were cancelled. I was in downtown Honolulu at 3:00 or so. All the shop windows were taped up, and a cold, dry breeze blew through the streets, picking up bits of paper and carring them around. There was not another soul on the streets, and I was not

able to get back to the base, as all the buses had stopped. I eventually got someone to come down and pick me up, and we were the only car on the roads. I don't know much about the damage to Honolulu, being stuck on base for a while because I had no form of transportation (tree fell on car).

> [This could be a separate story in itself, but suffice it to say that the
> Civil Defense Emergency Broadcast system didn't work. Besides all the TV
> stations, all the radio stations---except one--- went off the air that
> night. The single radio station that had an operating emergency generator
> was running "on automatic", playing religious music.]

Nope. Radio station KGU was on almost all the time, on their standby generator. They were off for a few hours when their antenna was damaged, but brought the transmitter (at the studio site) back up with a long wire dipole. At first they were calling various authorities, but after the phone went out, they just sat around and played music, complaining about the weather.

I don't think that the extent of the damage to the military installations was ever revealed, so you can probably say you saw it first here. It doesn't have much to do with risks from computer systems, but it does have a bit to do with risks to computer systems, as well as anything else that uses electricity. At least, I know my PDP-11 did go down at the time.

Scott Dorsey Kaptain_Kludge ICS Programming Lab, Rich 110,
Georgia Institute of Technology, Box 36681, Atlanta, Georgia 30332
...!{akgua,allegra,amd,hplabs,ihnp4,seismo,ut-ngp}!gatech!gitpyr!kludge

Search RISKS using swish-e

THE RISKS DIGEST

Forum on Risks to the Public in Computers and Related Systems

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

Volume 4: Issue 53

Sunday, 1 March 1987

Contents

From: "Lindsay F. Marshall" <lindsay%kelpie.newcastle.ac.uk@Cs.Ucl.AC.UK>
Date: Fri, 27 Feb 87 13:52:19 gmt
To: risks@csl.sri.com
Subject: Setuid Patent

Can we knock this one on the head once and for all? The patent for this did exist but was allowed to lapse by AT&T. The proper use of setuid is of course NOT nonsecure and does allow the easy implementation of certain facilities. Badly used, yes it can be nonsecure, but don't knock it because of that!!

Lindsay

> [It is precisely BECAUSE it allows easy implementation that it is so frequently misused -- by people who don't know better. Use of "setuid" opens up the possibility of a variety of security flaws, including Trojan horses, search-path traps, etc., and tends to substantially widen the perimeter of trust. I'm not sure that anyone knows how to characterize "proper use" completely -- if

it is indeed possible at all. PGN]

On PGN's editorial comment on human misuse of computers

Eugene Miya <eugene@ames-nas.arpa>
Fri, 27 Feb 87 09:43:48 PST

I read this today and wonder if I would really regard this as a risk. We have Use, Abuse, and Misuse. I sometimes (emphasis) like to believe that the last two are not possible -- that a different word is needed. Yes, I acknowledge that the Mafia can use dBase II, or the people at kremvax use Lotus on separate PCs ;-).

Remember: light behaves like a particle on MWF and a wave on TTS. This might be a useful technique.

--eugene miya
NASA Ames Research Center

[We also include part of Eugene's respose to Brian Randell:]

To: brian%cheviot.newcastle.ac.uk@cs.ucl.ac.uk
Cc: risks@csl.sri.com
Subject: Re: RISKS and human errors
Date: 27 Feb 87 11:08:07 PST (Fri)
From: eugene@ames-nas.arpa

What a wonderful thing to see:

> Today I telephoned Prof Reason, and had a very interesting chat with
> him. We have arranged that he will come and give a talk ...

It upholds some faith in the value of television.

You might ask Dr. Reason [interesting name] about the role in the past of things such as ritual, mnemonics and (devices) [programmes] as this was the way things were done in the past before writing, and it also probably helped with the development of such arts as poetry. I think this is important (if you have not realized this) because of proposals for nuclear waste include monuments and the creation, literally, of a "priesthood" to deal with nuclear waste. Could similar such priesthoods develop for computers (some would say we have such now)?

A follow-up report on Dr. Reason's seminar would be most interesting.
I wish I could attend. Thank the net.

--eugene miya, NASA Ames Research Center

[The 19th Century English characturist Thomas Rowlandson had a favorite character named Dr Syntax -- who somehow still seems relevant today.

By the way, I wanted to close the loop on Eugene's comment, "I think an

apology is in order", and MY apology in RISKS-4.52. Eugene's subsequent reply suggests that maybe I overreacted to HIS comment -- HIS later response suggests (rather modestly) that the original comment might have been intended to imply that HIS apology was in order. But that was much too kind of him. (A still later comment from him could be interpreted still differently, so I'll just leave it the way it was in RISKS-4.52.)
PGN]

An aside on the B-1

Eugene Miya <eugene@ames-nas.arpa>
Fri, 27 Feb 87 10:44:29 PST

Sigh! This hits home. When I was in high school, I had a job with North American Rockwell designing parts for the B-1 after school. Three stiffeners are mine. It was always interesting to be sitting trying to figure out how to design something when some one would walk in with a requirement for a hole (right there). Why? Avionics. Nothing more would be said. You were not supposed to ask as an airframe person. Interesting to see that all this comes back to the avionics people.

[This provides an interesting lesson to programmers who don't understand the environment in which a program is expected to run.
In response to my query of Eugene on "stiffeners", he replied thusly:]

Angle brackets used in homes are stiffeners. They fit into corners to make the structure more rigid. Interesting asides: there are two philosophies in building aircraft. (I was told this as a young engineer, and I passed it on the space group recently WRT multi-piece SRB design.) You make can make aircraft from a few large pieces, or from many small pieces. Boeing is a big pieces company and Rockwell (my ex while in HS) was a small-pieces company. Tradeoffs in both directions: like multics and unix, pl/1 and c.

--eugene

Autolander discussion

Nancy Leveson <nancy@ICSD.UCI.EDU>
27 Feb 87 15:20:45 PST (Fri)

I am a little confused about all the recent discussion in Risks about pilot problems with autolanders, etc. I read a paper written in the early 70's about how the autolander for the L1011 was verified. So there are already autolanders in operation and have been for a long time. Yes, they use analog computers rather than digital computers, which makes a difference in implementation techniques and perhaps reliability, but should make no difference from the pilot's point of view. Perhaps I am missing something here? Does a digital autoland system perform different functions than an analog one?

Re: Air Traffic Control, Auto-Land (RISKS DIGEST 4.51)

Dean Pentcheff <dean%violet.Berkeley.EDU@berkeley.edu>
Wed, 25 Feb 87 21:48:55 PST

I would be equally unhappy being a passenger in an autolanding plane as I would be living in a chronic state of "launch-on-warning" nuclear policy. In either case the machinery makes the ongoing critical decisions, and the people supervising it just *might* be able to notice a problem, acquaint themselves with recent system actions, and make the appropriate correction (if still possible). In indeterminate, complex situations such as strategic nuclear systems and plane landings, I am much happier if the (admittedly fallible) humans are making the ongoing decisions, with a possibility that machinery might notice a problem and warn them. The "supervisors" stand a much better chance of being able to react appropriately to an unexpected situation if they have the "feel" of the system by already having been in control of it.

-Dean (dean@violet.berkeley.edu)
-University of California, Berkeley Department of Zoology

[The home of nonviolet resistance and inviolet principles! PGN]

Electronic Steering

Ray Chen <chen%gt-stratus%gatech.csnet@RELAY.CS.NET>
Thu, 26 Feb 87 23:06:09 EST

Miliary aircraft not only get maintained more often than the average car, but they are also designed and manufactured to more exacting and demanding specifications than their civilian counterparts. Military hardware in general is designed to operate correctly in wider range of operating conditions and more thoroughly tested.

Military software must also meet certain coding standards and go through formal verification testing before being approved.

Now, none of this guarantees that all errors are caught (especially the software errors). You do, though, have some guarantees about whatever can be tested properly such as component quality, and RFI-shielding.

Given the amount of testing and verification a MIL-spec steer-by-wire car would have to endure before being accepted, I might consider driving a steer-by-wire car with software that had been coded and tested under military specs and ran on MIL-spec, RFI-shielded hardware.

Given the history of electronic ignition systems however, I wouldn't come near a steer-by-wire car that had been developed and manufactured to "GM-specs".

Ray Chen

Electronic steering

<LIN@XX.LCS.MIT.EDU>
Sat, 28 Feb 1987 12:54 EST

We pay fighter pilots to take large risks. Furthermore, combat jets are not generally regarded as the ultimate in safety, since they sacrifice a lot to get high performance.

[OK, gang, that is probably enough on this topic for now. Thanks. PGN]

Search RISKS using swish-e

THE RISKS DIGEST

Forum on Risks to the Public in Computers and Related Systems

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

Volume 4: Issue 54

Monday, 2 March 1987

Contents

Rockford Illinois Destroyed by Computer!

<Chuck.Weinstock@sei.cmu.edu>
2 Mar 1987 19:27-EST

According to the CBS Evening News, the National Weather Service issued a report that Rockford Illinois was destroyed by a killer tornado this morning. The report was picked up by the media and reported as fact. Rockford is still there, the NWS was just testing a new reporting mechanism. The report should not have been issued. The NWS blames faulty computer software.

Ma Bell's Daughter Does Dallas

Peter G. Neumann <Neumann@CSL.SRI.COM>

Mon 2 Mar 87 14:32:52-PST

The Number 4 ESS system in Dallas went down for much of the day on Wednesday, 25 February 1987, blocking most long-distance calls in and out of area code 214. Both the main system and the backup system failed. One smart company was Fidelity Investor Information, which was able to reroute incoming calls (presumably through an 800 number?) to phone centers in Boston and Salt Lake City. Multilevel layers of redundancy seem like a good practice. [Source: Austin American Statesman, 26 Feb 87, p. D11, courtesy of Steve Smaha, by SnailMail.]

> [Although presumably not computer related, a highly toxic fire broke out at 3 a.m. on 18 Feb 87 in a Brooklyn NY Tel central office, downing 5 exchanges and 41,000 customers. Because of the toxicity levels, repair personnel were not allowed in the building until after 5 p.m. During the same week, a Chesapeake & Potomac switching center also experienced a toxic fire, forcing evacuation on two consecutive days. See Management Information Systems Week, 23 Feb 87, p. 31 and 54 for details.]

FAA Does Houston

Peter G. Neumann <Neumann@CSL.SRI.COM>
Mon 2 Mar 87 14:39:18-PST

The computer complex at the FAA's en-route traffic control center in Houston went down at 7:13 a.m. on Tuesday, 24 February 1987. Primary radar was restored at 7:45; the manual backup system was in effect throughout the outage. The computer system came back up at 10:40 a.m. Delays of 90 minutes for commercial flights were reported, affecting airports in the surrounding multistate area. [Source: UPI, from SF Chron, 25 Feb 87, p. 3.]

Tempest Puget, or The Sound and the Ferries

Peter G. Neumann <Neumann@CSL.SRI.COM>
Mon 2 Mar 87 15:08:44-PST

In this decade there have been at least a dozen dock crashes in the Puget Sound ferry system (the largest such system in the USA) that were attributable to onboard computer failures. The damages for one crash alone (12 September 1986) cost an estimated $750,000 in repairs to the Whidbey Island dock. The $17 million mid-sized Issaquah ferries [100 cars, 1200 passengers] came on board in 1980 with the slogan, "Computerized propeller systems make the ferries more fuel efficient." The state sued the ferry builder (the now bankrupt Marine Power & Equipment of Seattle), which agreed to pay $7 million over 10 years. The state's recommendation now is to spend an extra $3 million cutting 6 ferries over to MANUAL CONTROLS.

[Source: An article by Deeann Glamser in USA Today, 25 Feb 87.]

> [It is disappointing that the fix is to bypass the computer systems, rather than to make them work. Nevertheless, accepting reality is

clearly a good idea. Although they did not have a gift horse in whose mouth to look, perhaps Seattle still believes in the truth ferry.]

Re: proper use of suid

Jef Poskanzer <unisoft!charming!jef@ucbvax.Berkeley.EDU>
Mon, 2 Mar 87 09:45:06 PST

Proper use of suid is easy to characterize: don't use it, use sgid instead! If you need complete security, set up a separate group for each separate application, make the files it needs access to writable by that group, and you're set. [with sgid]

Jef Poskanzer unisoft!jef@ucbvax.Berkeley.Edu ...ucbvax!unisoft!jef

---

Process Control

<Chuck.Weinstock@sei.cmu.edu>
2 Mar 1987 19:30-EST

I had the good fortune to tour General Electric's Grove City, PA diesel engine manufacturing plant on Friday. The plant manager, who was conducting the tour, was especially proud of the highly automated machine tools and the computerized engine testing cells. They are so confident of the process-control computers' ability to detect problems that the employees in charge of watching the process are allowed to take a break while things keep running. I found this appalling. The fact that the test cells were made of reinforced concrete to shield the rest of the facility from an engine explosion did not make me feel any better.

The plant is currently running at less than one third of capacity. I wonder what surprises they are in for if and when it starts running at or near capacity?

Risks in switching to computerized `people meters'

Bill Janssen <janssen@MCC.COM>
Mon, 2 Mar 87 15:50:10 CST

The March 2, 1987, issue of the `New Yorker', has a discussion of `people meters' in its editorial column. The two major television audience-rating companies, Nielsen and AGB, are each going to switch from a paper-and-pencil diary system of recording viewing samples, to an automatic electronic system that is connected to the viewing family's television sets and VCRs.

There will be some measurement effects: ` ``Here's something that causes us concern, '' Mr. Dominus (a vice-president of CBS) stated. ``To install this system, a man has to wire your house. Let's say you've got two sets and a VCR. He has to literally solder stuff to your equipment.

When you walk into the room and turn on the set, you have to punch in, and when you go out of the room you punch out. I would say there's a personality bias toward people with a high-tech style. Now, some people are technology-adverse -- I'm one of them, so I ought to know. They say, `I don't want to do this.' How do you adjust for that mind-set?" '

Apparently the advertising agencies will want `a money-back guarantee that a given commercial would reach a givena number -- and type -- of viewer.' The networks, because of the unknown nature of the measurement effects, want to avoid giving such guarantees, particularly on $3.7G worth of business, the amount of up-front advertising that was sold last year. They would like to forego guarantees this next year to `save the networks a fortune in unfairly assumed risk.'

Toward the end of the article it is revealed that the actual system under discussion is a `real-time electronic diary', instead of a true `people meter', which would function in a totally passive way, leaving no room for human error (such as forgetting to punch in). `Computerized voice identification' and `miniature radio transmitters built into the family jewelry' are mentioned as research directions...

Bill

A lovely algorithm

<LINDSAY@TL-20B.ARPA>
Sun 1 Mar 87 22:19:25-EST

Occasionally, one encounters a truly lovely algorithm. Often they can be recognized by their simplicity.

A friend of mine discovered such an algorithm on the Burroughs 6700, lo these many years ago. It all came about because he was debugging a database manager. One day, it attempted to use a somewhat random number as in index into a data file.

Now, my friend had a budget, and received bills monthly from the computer centre. The next bill was shocking, and in fact, wasn't even believable. He had been charged for more disk space than the centre owned.

It was obvious that the billing software didn't really know how large the files were. Instead, the biller trusted each user program to end at the end of its file. In the true spirit of experimental science, my friend changed his program so that it would always finish by accessing at index zero.

And indeed, on the next bill, he was charged precisely zero for disk space.

Report problems with the web pages to the maintainer

Search RISKS using swish-e

THE RISKS DIGEST

Forum on Risks to the Public in Computers and Related Systems

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

Volume 4: Issue 55

Tuesday, 3 March 1987

Contents

Air Cargo system in chaos (from The Times)

"Lindsay F. Marshall" <lindsay%cheviot.newcastle.ac.uk@Cs.Ucl.AC.UK>
Tue, 3 Mar 87 16:31:57 GMT

A computer system, installed at airports to help to speed cargo deliveries, has been withdrawn from service after it collapsed as soon as it was switched on (Our Air Correspondent writes).

Now cargo agents are considering taking the airlines which own the computer to court because, they claim, they have lost up to 5million pounds as a result of the failure.

The computer was installed by travicom, a company jointly owned by British Airways and British Caledonian.

After a meeting of more than 100 freight forwarding agents yesterday Mr. Chris Quintin of the cargo company LEP said: "The system was simply unable to cope with the requirements we put on it. As a result cargo and freight was held up all over the country, diverted from one airport to another and couldn't clear Customs because they were plugged into it too."

Travicom has offered 500,000 pounds.

ATM Cards Devoured (again!); Royal Shakedowne for Tickets

Robert Stroud <robert%cheviot.newcastle.ac.uk@Cs.Ucl.AC.UK>
Tue, 3 Mar 87 17:18:24 GMT

(1) Yesterday (2nd March) the bank machine swallowed my card when I asked for some money, claiming that it had expired. Not having checked the date beforehand I didn't know if this was true or not, but I hadn't received a replacement card in the post in advance which usually happens.

When I cashed a cheque today in my branch and complained about this, I was told that I was not alone. All the cards for customers of the branch which were due to expire in June had expired in February instead although the computer wasn't planning to send out the replacements until June. I assume that there was a discrepancy between what was printed on the front of the card and what was encoded in the magnetic strip on the back.

(I got the impression from the cashier that all the cards issued by the branch expired on the same date {June} so that the problem was actually quite serious. However, there didn't seem to be many irate customers about, and people were using the machine outside {although possibly with cards issued by different branches}, so maybe I was mistaken in this impression.)

(2) Every year the Royal Shakespeare Company brings their current productions to Newcastle before taking them to London. This year the Theatre Royal has acquired a nice new computerised booking system that prints your name on the ticket and lets you choose where you want to sit on the screen.

[I hate sitting on screens. The electrostatic effect is annoying. PGN]

When I went in about a week ago to try and get some tickets for one of the productions, I was told that although there were plenty of seats available, I couldn't buy any tickets because the computer was down. (However, I was able to get a couple of returns for Midsummer Night's Dream the old fashioned manual way). Apparently the machine was still broken several days later so they can't have been able to sell any tickets in the meantime - it

is perhaps just as well that the Shakespeare productions are usually sold out months in advance.

Robert Stroud, Computing Laboratory, University of Newcastle upon Tyne.
ARPA robert%cheviot.newcastle@ucl-cs.ARPA UUCP ...!ukc!cheviot!robert

[They won't be sold out months in advance if that keeps up! PGN]

Re: Risks in the NSC computer archives

Carlton Hommel <carlton@masscomp.UUCP>
2-Mar-1987 09:16-EST (Monday)

The columnists Evans & Novak were interviewing Gen. Brent Scowcroft on their CNN show Sunday. They asked him if the information retrieved from the NSC computer archives provided data that was not found anywhere else. He replied no -- they would have been able to track it down from other sources. However, it was instrumental in showing that North was not working in a vacuum -- there were on-line copies of memos that he wrote to higher-ups, keeping them informed of his activities.

Carl Hommel
{allegra, bellcore, cbosgd, decvax, gatech, seismo, tektronix}!masscomp!carlton

---

Re: A Scary Tale--Sperry Avionics ...

Kevin Driscoll <ames!rutgers!mmm!SRCSIP!kevin@cad.Berkeley.EDU>
Tue, 3 Mar 87 02:15:13 CST

You know that I am not a fan of N-version programming. However, I must say that the tale is not as scary as might have been implied by the "man at the FAA". Sperry Avionics was recently purchased by Honeywell and I have been working with the people who are advocating this N-version approach. The following is my own opinion and not that of my employer ... etc.

What Sperry wants to do is use N-version software in place of "white box" (structural) tests. The "black box" (functional) tests would be still be performed. Specifically, Sperry has asked the FAA for concurrence on using the N-version techniques described in Larry Yount's 1984 AIAA paper 84-2603 and Level 2 software V&V {referring to RTCA/DO-178A, which uses 3 levels of software (depending on criticality): Level 1 (Critical), Level 2 (Essential), Level 3 (Non-Essential)}.

In its letter to Sperry, the FAA says that this method "appears to be satisfactory" with the following constraints:

a. Level 1 must used for paragraphs 6.2.2 (Requirements Development and Verification) and 6.2.3 (Design).
b. Formal configuration control must used and, if common errors are found, structural testing may be required for some or all of the modules.
c. Formal review and comparison of source code must be used to verify dissimilarity. Where this is not feasible, Level 1 structural test and

analysis must be used.
d. Functional tests of the system must be performed. It must be shown that the system will not have false alarms.

It seems to me that c. is the same as doing structural analysis. Therefore, this method is not any less rigorous than "full" DO-178A Level 1. However, how one complies with c. and d. I do not know.

Kevin R. Driscoll, Senior Research Scientist (612) 782-7263
Honeywell, 3660 Technology Drive, M/S MN65-2500, Mpls, MN 55418
UUCP: {ihnp4,philabs,umn-cs,mmm}!srcsip!kevin

Re: Altitude encoders: $1500 for Mode C? No, $750.

Jordan Brown <jbrown@jplpub1.uucp>
3 Mar 87 06:10:40 GMT

We just had an altitude encoder installed in our airplane for $750...
I strongly recommend that any A/C owners out there get one.

One more on fly/steer-by-wire

<rutgers!jhc@mtune.ATT.COM>
2 Mar 87 22:58:55 EST (Mon)

I think that it is relevant to point out that pilots of military jets have a very good record of steering a broken plane so that it crashes in a safe area, sometimes at the cost of their own lives. How many of us would do the same in a car? Also, all the rear-wheel steer-by-wire systems which I have heard about have been designed to be fail-safe, by locking the rear wheels in the straight-ahead position, which makes them the same as current-day cars. Should they fail in a locked-over position then the driver would feel some steering drag, but nothing uncontrollable. Some show vehicles have had full steer-by-wire, but this is at no more than the experimental stage.

Jonathan Clark jhc@mtune.att.com

Steer-by-wire cars (Re: RISKS DIGEST 4.53)

Doug Rudoff <doug@wiley.UUCP>
4 Mar 87 00:56:12 GMT

Concerning steer-by-wire cars, why would you want one in the first place ? I can understand the use on a large airplane where it would be almost impossible to fly without some sort of power system. But with a car, where it seems that it easy to have direct mechanical linkage for steering as well as a power system, why bother ? It's also probably safer that way too. Mechanical linkage steering does not have a very high incidence of failure.

Doug Rudoff TRW Inc., Redondo Beach, CA !{trwrb,cit-vax}!wiley!doug

Software Safety in ACM Computing Surveys, June 1986

Daniel S. Conde <conde@granite.DEC.COM>
Tue, 03 Mar 87 16:19:25 -0800

The June 1986 (that's right, 1986) issue of the ACM Computing Surveys just came out, and has an article by Nancy Leveson titled

"Software Safety: Why, What, and How".

It should be of interest to all RISKS readers. Dan Conde

Computerized `people meters' for TV audience ratings

Niall Mansfield <MANSFIEL%EMBL.BITNET@wiscvm.wisc.edu>
Tue 3 Mar 87 11:54:57 N

As far as my sketchy knowledge goes, the audience ratings here in Germany are collected (or soon will be) by true 'people meters'. A box with phone line access is hardwired into the TV, and it detects and records what channel is being viewed when. The central data collection office dials up each viewers' meter overnight, and the data are sucked up for processing. The one thing the box can't do is know who is actually looking at the TV; for this a hand-held thingummy (rather like a TV remote control) is supplied, which has a button for each member of the family (and and extra one for visitors - isn't that very hospitable of them!). People are supposed to 'clock in' and out their personal viewing with the buttons.

Personally I wouldn't be caught dead with such a thing. Big Brother would have to do almost nothing to monitor an awful lot of your life, almost in real time.

More on Dallas phone outage

Mike Linnig <LINNIG%ti-eg.csnet@RELAY.CS.NET>
Tue, 3 Mar 87 08:55 CDT

(Ft. Worth Star Telegram -- STARTEXT (c) 26-feb-87)

AT&T computer failure stalls area 214 calls

DALLAS (AP) -- Long distance telephone service was back to normal Thursday in Dallas and across a vast area of North Texas after thousands of calls were blocked for hours because of a computer problem, an AT&T spokesman says. "Our number four electronic switching system, which is essentially a

large computer that switches long-distance clals into and out of the 214 Area Code, failed," Diane Schwilling, media relations manager for AT&T, said Wednesday. "The machine handles between 500,000 and 600,000 in its busiest hours. It's capable of handling more than that," she said.

The problem began about 9 a.m. Wednesday and by 2 p.m. the company had begun processing calls through the switch again. "From about 3 to about 4 it was handling calls real well," Ms. Schwilling said. Then, there were more problems. At 6 p.m., she said service was near normal and that no other work on the computer was planned for Wednesday night. The malfunction affected long-distance calls primarily into and out of the 214 area, so anyone calling into or out of the area could have been affected, she said.

"Other parts of Texas may have gotten more busy signals than normal simply because during the busy hours of the days, the Dallas switch acts as a backup and would pick up overflow traffic from other parts of the state," Ms. Schwilling said.

Soliciting suggestions for 1988 CSC panel on liability

Gene Spafford <spaf%gatech.csnet@RELAY.CS.NET>
2 Mar 87 13:59:41 GMT

For the program committee for the 1988 ACM CSC to be held in Atlanta, I'm organizing a panel session on liability issues in software. The intent is to have the panel address issues more related to the legal aspects rather than methods of software engineering methods or ethical considerations of using computers, although those also may be fair game.

I'd appreciate suggestions from Risks readers as to people you'd like to see on the panel. Please include some reasons why you think the people you are nominating would be interesting, and provide me with a contact address, if possible. You can nominate yourself if you believe you have something to contribute.

I already have some ideas of people to invite, but I'd like to get more input before issuing formal invitations. Thanks.

Gene Spafford
Software Engineering Research Center (SERC), Georgia Tech, Atlanta GA 30332
CSNet: Spaf @ GATech ARPA: Spaf@gatech.EDU
uucp: ...!{akgua,decvax,hplabs,ihnp4,linus,seismo,ulysses}!gatech!spaf

[Aha! RELIABILITY must be when you have LIABILITY and so you do it AGAIN. PGN]

Conference on computing and society in Seattle, preceding AAAI

Jon Jacky <jon@june.cs.washington.edu>
Tue, 03 Mar 87 08:59:31 PST

(Excerpts from call for papers in RISKS-4.28. Due date 4/1 is approaching.)

DIRECTIONS AND IMPLICATIONS OF ADVANCED COMPUTING
Seattle, Washington July 12, 1987

The adoption of current computing technology, and of technologies that seem likely to emerge in the near future, will have a significant impact on the military, on financial affairs, on privacy and civil liberty, on the medical and educational professions, and on commerce and business.

The aim of the symposium is to consider these influences in a social and political context as well as a technical one. The social implications of current computing technology, particularly in artificial intelligence, are such that attempts to separate science and policy are unrealistic. We therefore solicit papers that directly address the wide range of ethical and moral questions that lie at the junction of science and policy.

[Submit papers to be refereed on] RESEARCH FUNDING, DEFENSE APPLICATIONS, COMPUTING IN A DEMOCRATIC SOCIETY, COMPUTERS IN THE PUBLIC INTEREST, other relevant topics. The program committee includes Andrew Black (U. WA), Alan Borning (U. WA), Jonathan Jacky (U. WA), Nancy Leveson (UCI), Abbe Mowshowitz (CCNY), Herb Simon (CMU) and Terry Winograd (Stanford).

Complete papers, not exceeding 6000 words, should include an abstract, and a heading indicating to which topic it relates. Papers related to AI and/or in-progress work will be favored. Submissions will be judged on clarity, insight, significance, and originality. Papers (3 copies) are due by April 1, 1987. Notices of acceptance or rejection will be mailed by May 1, 1987. Camera ready copy will be due by June 1, 1987. Proceedings will be distributed at the Symposium, and will be on sale during the 1987 AAAI conference.

For further information contact Jonathan Jacky (206-548-4117) or Doug Schuler (206-783-0145). Sponsored by Computer Professionals for Social Responsibility, P.O. Box 85481, Seattle, WA 98105.

Search RISKS using swish-e

THE RISKS DIGEST

Forum on Risks to the Public in Computers and Related Systems

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

Volume 4: Issue 56

Thursday, 5 March 1987

Contents

Computer problems produce false weather warnings

Mike Linnig <LINNIG%ti-eg.csnet@RELAY.CS.NET>
Wed, 4 Mar 87 15:16 CDT

From: Ft. Worth Star Telegram, STARTEXT, Mar-4-1987

Computer problems produce false weather warnings

WASHINGTON (AP) -- The National Weather Service ordered a halt to all test warnings on its national weather wire Wednesday, until corrections can be made in new computer programs that have led to several false warnings in

recent days. "A cease and desist on all drills has been ordered until we can correct the system," spokeswoman Carolyn DeBona said in a telephone interview.

Two false warnings were issued in the Chicago area and others occurred in Brownsville, Texas; Long Island, N.Y.; and Washington, D.C., said another Weather Service spokesman, Donald Witten. And reports of a similar problem on Tuesday have been received from Dodge City, Kan., officials said.

Witten said the troubles started after local Weather Service offices were sent new computer programming discs designed to speed warnings when severe weather conditions occurred. The discs include prepared messages, with local forecasters only required to fill in the names of endangered cities or counties and provide any necessary localizing information, he said.

When the meteorologists tried out the new discs, they were supposed to include the statement "This is Just a Test," but for some reason that phrase did not get transmitted in several instances, Witten said. He said Weather Service programmers are currently analyzing the discs to see where the problem is located and to correct it, a process that could take a few days.

In the most widely publicized instance, a tornado warning was issued early Monday morning stating, incorrectly, that a twister had destroyed the city of Rockford, Ill., and was headed for Chicago. The statement was broadcast on several radio stations in the Chicago area before a correction was issued. A severe thunderstorm warning -- also false and also without the "test" disclaimer -- was transmitted at 1:53 p.m. Monday from the Chicago Weather Service office and also had to be corrected.

In the Long Island case, the warning from the New York City weather office occurred the afternoon of Feb. 20 and involved a tornado warning for Nassau County, N.Y., and two New Jersey counties, according to local news media. That tornado statement was followed by a message 16 minutes later that said the original warning had been in error.

The Brownsville case occurred at 8:41 a.m. Monday and also involved a tornado warning, according to Weather Service officials.

In the Washington instance, on Sunday, a severe weather warning was issued at 2:32 p.m.

In Dodge City, the false bulletin reported a tornado near Medicine Lodge and moving northeast. Five minutes later, the Weather Service sent a disclaimer saying the bulletin had been sent by mistake.

Jim Johnson, a meteorological technican who was on duty when the false bulletin moved, said he was testing a new computer program used for severe storms forecasting when the bulletin was accidentally transmitted.

The warnings are distributed on the agency's "weather wire," a Teletype circuit that prints out local conditions, forecasts and warnings. Local Weather Service offices issue their reports on this wire, which is widely used by the news media, government agencies and others.

Some postscript notes about Hurricane Iwa

<CUNNINGHAMR%HAW.SDSCNET@nmfecc.arpa>
Thu, 5 Mar 87 08:43:21 PST

To the best of my knowledge, the outage of one of the working GOES satellites (summer 1983) was from causes which are still unknown, onboard computer being a possibility. (Do any other RISKS readers have more information on this?)

The decision to have the remaining GOES cover just the Atlantic was definitely an "assumption of risk" on the part of the National Weather Service, based on a decision that it was more important to accurately hurricanes and other weather affecting the U.S. east coast.

After Hurricane Iwa, the NWS had the GOES "cheated" west to be able to just see the Hawaiian islands, and found they could get some coverage of the central and western Pacific from a Japanese GOES-like satellite and miscellaneous polar orbiting satellites. Most of that info was presumably also available back in 1983...but not used by the NWS at the time of Iwa.

GOES-7 was finally launched successfully last week and---after many delays and one splash since 1983---the NWS finally has separate GOES capable of monitoring weather over both the Atlantic and Pacific oceans, with overlap coverage of North American.

However, it is still an open question whether better satellite coverage, giving a more accurate track of Iwa, would really have had much effect.

The complete story of the effects of Iwa can (and did in subsequent government investigations) fill volumes. A useful case study for anyone interested in natural disasters in general. Perhaps also an interesting study of the failure modes of different types of interdependent systems (EBS, telephone system, water, sewage, city gas, transportation, food supply) when a major system (electrical) upon which others depends, fails suddenly.

For example, some of the "pre-programmed" contingency plans that were activated weren't appropriate. After the initial serious alert went out on the radio stations just before noon on Thanksgiving the bus system continued in normal operation until approximately 2:00pm (during the worst traffic jam in Honolulu's history), the bus company then activated the only emergency plan they had, for tsunami/earthquake evacuation. All running buses proceeded to previously-designated schools in the hills with reinforced concrete buildings. However, since it was Thanksgiving, the schools were closed, leaving confused bus riders to walk home from wherever they happened to end up.

After Iwa, the Civil Defense groups (both state and county) were completely re-organized, and a emergency radio communications network (yet to be tested under realistic conditions) has been set up to reduce CD's dependency on both the telephone system. CD has also added a collection of microcomputers to keep track of things and beefed up their uninterruptible power supply (UPS) systems.

The major electrical utility, Hawaiian Electric built a new centralized, highly computerized monitoring and control facility (itself protected by a rather large UPS) for the electrical grid on the island of Oahu. One of the reasons: a second failure of the electrical grid 9 months or so after Iwa when a fire which brought down a transmission line, the resulting surge burned out a key relay, and isolated the major generators.

Hawaiian Electric now claims that type of failure won't happen because their new computers "react faster than people".

[By the way, let me take this opportunity for an erratum. The contents

list in RISKS-4.51 should have attributed the original message in this sequence as follows:

Hurricane Iwa and the Hawaii blackout of 1984
(Bob Cunningham responding to James Burke, via Matthew P Wiener)

PGN]

Tempest Puget

Bill Roman <sigma!roman@entropy.ms.washington.edu>
Wed, 4 Mar 87 08:05:54 pst

RUMOR

I can't vouch for this personally... but a few years ago I spoke to a contractor who said he had been approached to write software for the Issaquah class ferries. According to him, there were single-chip microcomputers in the wheel house and in the engine room which communicated by direct connection of their serial I/O pins. No buffering. So, apparently, when the captain moves the engine controls on the bridge, the engine computer is all too likely to reply "what's that Captain, I canna hear ye."

My friend refused the contract.

Computer Aided Dispatching (again)

James Roche <roche@rochester.arpa>
Thu, 5 Mar 87 08:14:20 est

The continuing saga of the Rochester/Monroe County 911 dispatching center continues. The following was printed in the Saturday 2/28/87 Democrat & Chronicle:

A 911 computer error sent sheriff's deputies to Hilton instead of Spencerport yesterday afternoon said Sgt. Paul Hayes of the Monroe County Sherriff's Department. A caller to 911 said there was an assault taking place at 111 West Ave., then hung up, Hayes said. A computer readout indicated the call had come from Hilton, but when deputies arrived at 5:25 p.m. they could not find number 111.

The 911 center called back the number on the computer readout, which was correct, and found that the call had come from West Avenue in Spencerport. A deputy arrived at the scene at 5:28 p.m. Hayes said.

"Apparently the computer's program is somehow at fault", he said.

The incident was over when police arrived. There were no injuries he said.

Jim Roche University of Rochester Computer Science Dept Rochester, NY 14627
ARPA: roche@rochester.arpa, UUCP: rochester!roche

<"guthery%asc%slb-doll.csnet@relay.cs.net">
Wed, 4 Mar 87 07:40 EDT

<"ASC::GUTHERY%slb-test.csnet"@RELAY.CS.NET>
To: risks@CSL.SRI.COM
Subject: Teflon flywheels and safe software

When a computer-based misfortune occurs, we are quick to fault the last-in-line of the system builders. Usually this is what is euphemistically and disparagingly called the applications programmer. Only on rare occassions do we ask if this unfortunate soul could have done any better given the tools that were available. Consider ...

Modern computer architectures (the Transputer, for example) sacrifice time determinism in favor of speed. Modern computer languages (Ada and Occam, for example) sacrifice time determinism in the interest of features (Ada) or provability (Occam). And yet, the metaphorical mist that surround these developments (concurrent, multi-tasking, real-time, etc.) invites people to incorporate them in time deterministic systems like cars and planes. As if the applications programmer didn't have enough to worry about, he now has to build a deterministic system using a non-deterministic language on top of a non-deterministic machine.

What I'm getting at is that while we all talk about risk reduction, not only do we not specify and build system components (machines, languages, theories, test harnesses, diagnostic tools) that let us get ahold of and engineer risk factors, we encourage, yea verily demand, components that are ever more slippery. Then we give these teflon flywheels and greased gears to the application programmer and expect him to build a nice safe system.

How come my vendor won't tell me the instruction execution times of his machine? Where are the time specifications for an Ada kernel? Why are there no real-time languages? How come we don't insist on time delay guarantees for operating system calls? Why can't I turn off ALL interrupts? Why are time services so impotent? What exactly is the caching algorithm and how can I change it? Why can't I install my own scheduler? All these and many more.

If we want to really want to build reduced risk systems, then we should start to define and build reduced-risk parts. I don't believe you can expect the painter to be responsible for the structural integrity of the bridge.

[This a very nice challenge, and one that should be taken seriously. PGN]

<hplabs!cae780!amdcad!sun!nescorna!marcum@ucbvax.Berkeley.EDU>
Mon, 2 Mar 87 16:11:18 PST

(Alan M. Marcum)

To: amdcad!CSL.SRI.COM!RISKS
Subject: Autoland and Conflict Alert

First on autoland, there are various commercial planes flying that have an autoland capability, including the L1011, 767, 757 (this is not an exhaustive list). This isn't meant to imply that I approve or disapprove, simply that the system exists on a fair number of planes. In fact, the system was invented in England (CAT IIIC ILS approaches, in the jargon: ceiling 0', visibility 0 -- the stereotypical English day?), to help with some of the weather difficulties there.

Regarding Conflict Alert and Mode C transponders, this has been a topic of hot discussion of late. One recent comment on RISKS was to the effect that anyone owning a plane could afford the US$1500 or so to add Mode C. Many, many planes in the general aviation fleet have no on-board electrical system whatsoever, much less any transponder. A large number of pilots would find an additional $1500 a significant burden. Folks squawked about FAA's ELT (Emergency Locator Transmitter) requirement several years ago, and that was for much less than $1500!

It's unclear how much it would help right now, anyway, to require Mode C altitude reporting transponders on all planes (here's the competer tie-in, least you've been concerned). The current US ATC system (I'm unsure about that in other countries) would be grossly overloaded if all the planes in the sky now even had Mode A (position-reporting, without altitude), much less Mode C. This is a capacity limit of the computers and the signal processing equipment. Yes, they could be upgraded, and are being upgraded -- at tremendous expense (needed, perhaps), and it will take a long time.
--

Alan M. Marcum Sun Microsystems, Technical Consulting
marcum@nescorna.Sun.COM Mountain View, California

Re: Air Traffic Control, Auto-Land (RISKS-4.51)

Amos Shapir <decwrl!nsc!nsta!instable.ether!amos@ucbvax.Berkeley.EDU>
Thu, 5 Mar 87 11:34:41 -0200

>I would be equally unhappy being a passenger in an autolanding plane as
>I would be living in a chronic state of "launch-on-warning" nuclear policy...

Yes, automatic anything will have bugs and accidents will happen; however since we cannot eliminate them altogether, the question should not be whether automatic systems will cause accidents, but whether the accidents' cost would be greater os smaller than the cost of accidents in the human systems they replace. The type of accidents may be different, and some automatic systems introduce hazards were none were in a parallel human system; but they also solve many more problems than they introduce.

Amos Shapir
National Semiconductor (Israel), 6 Maskit st. P.O.B. 3007, Herzlia 46104 Israel
(011-972) 52-522261 amos%nsta@nsc.com 34.48'E 32.10'N

Re: An aside on the B-1

<pyramid!utzoo!henry@hplabs.HP.COM>
Tue, 3 Mar 87 17:07:20 pst

>...You can make aircraft from a few large pieces, or from many small pieces...

Ed Heinemann, famous for designing aircraft that were lighter and cheaper than anyone else thought possible, was a real fan of big pieces, because a structure of a given size needs *more* small pieces. He once said something along the lines of "when you count the parts in the F-14 wing, it's obvious why the F-14 is so expensive". I'd speculate that there is a correlation with reliability as well, again because of simplicity. Here we have an analogy to software in the opposite direction from the one Eugene was making: Unix builds things out of little pieces, but it is a big-piece system in one way because it emphasizes a few unifying principles rather than a myriad of special cases.

Henry Spencer @ U of Toronto Zoology
{allegra,ihnp4,decvax,pyramid}!utzoo!henry

Plane Crashes

David Purdue <munnari!csadfa.oz!davidp@seismo.CSS.GOV>
Thu, 26 Feb 87 16:20:45 est

I was told an interesting story last night, and I wonder if anything has been written about it in mod.risks, or if anyone knows anything about it (or even if it is true!).

In Europe there was a spate of (F-111?) crashes. The apparent cause of these crashes was pilots (1) believing they could fly the plane on their own without the help of any dumb computer, (2) turning the computer off, and (3) promptly flying into a mountain.

Any Hints? DavidP

Mr. David Purdue Phone ISD: +61 62 68 8165
Dept. Computer Science Telex: ADFADM AA62030
University College ACSNET/CSNET: davidp@csadfa.oz
Aust. Defence Force Academy UUCP: ...!seismo!munnari!csadfa.oz!davidp
Canberra. ACT. 2600. ARPA: davidp%csadfa.oz@SEISMO.CSS.GOV
AUSTRALIA JANET: davidp@oz.csadfa

In defense of drive-by-wire

Mike McLaughlin <mikemcl@nrl-csr>
Thu, 5 Mar 87 09:15:43 est

Numerous contributors have attacked automotive drive-by-wire systems. Consider some possible benefits, if implemented correctly:

- No more drivers speared by the steering column
- Speed-proportional steering
- Feedback selectable to match the individual driver's needs
- Easy to implement special controls for the handicapped
- Three degrees of freedom for "steering wheel" adjustment and for driver entry

Basically, "drive-by-wire" will allow unlimited freedom to human-engineer
the driver's input to the steering system of the automobile. I suggest
that we concern ourselves with ensuring that the system is safe and reliable,
instead of reminiscing about the good old days of mechanical steering.

- Mike McLaughlin

Search RISKS using swish-e

Report problems with the web pages to the maintainer

Search RISKS using swish-e

THE RISKS DIGEST

Forum on Risks to the Public in Computers and Related Systems

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

Volume 4: Issue 57

Friday, 6 March 1987

Contents

Re: Air Traffic Control, Auto-Land

David Redell <redell@src.DEC.COM>
Fri, 6 Mar 87 13:20:07 PST

Recent discussions have compared risks of computerized autolanding of planes to those of computerized launch-on-warning of nuclear weapons. I think lumping these together can be misleading. For example, as Mr. Shapir points out:

> ...the question should not be whether automatic systems will cause
> accidents, but whether the accidents' cost would be greater or smaller
> than the cost of accidents in the human systems they replace.

This is A good question, but not THE only good question. In cases where an existing situation is being automated, I agree that this is the right question to ask. Often, however, the prospect of using high-speed computer control is cited in support of plans to establish new situations where human control would be unworkable. Subsequent discussion often focuses on the

relative risks of human vs computer control. But if neither works, then the mistake is to get into the situation in the first place! Ideas like computerized launch-on-warning or AI-based weapons release for SDI are not bad ideas because humans could do those jobs better -- they are bad ideas because we are moving toward situations where neither humans, nor computers, nor any combination of the two can be trusted to do the right thing in the time available. One of our responsibilities as professionals is to try to identify and call attention to such situations before the choice degenerates to one of arguing about which of several unworkable options is the least unworkable.

Dave Redell

911, drive-fly by wire, risks, and the American work ethic

Wes Williams <eww@OBERON.LCS.MIT.EDU>
6 Mar 1987 1516-EST (Friday)

(interrelated thoughts)

911: Having been associated with the Emergency Services for some 20 years, I do not find the 911 articles surprising. I remember the horror stories from the times of conversion from "local" operators to those of the more regional type. People were accustomed to picking up the phone and yelling help or fire and screaming the address to the operator. While in the "new" system, the "0" DIALED in the phone would connect you to the local operator (usually) within the town or city of origin. Here the most severe complications were duplicate street names or same names suffixed by St. or Terr. or Place or Circle. As time went by the switchboards dissapeared from the local towards the regional type. Now the problems grew to the kind of identifying the neighboring community possibility. Here the operator would be the one in the position of determining the locality of origin of the call, as well as the correct address. Sometimes (1960's era to present) multiple community dispatches were heard for the same address in different municipalities.

The problems have not been rectified, only compounded by the advent of differing phone systems and overlays of telephone exchanges. Software may or may not be the problem, as the best software can only rely on input (electronic or manual). As area codes are becoming more and more prevalent, it may be necessary to soon dial an area code to report the fire across the street. hmmmmmm.....

Point 1. System modification (hard or soft) is not always the answer unless the root problem is solved. Even here, there will forever be unresolved complications. Example: a non-English speaking (obscure language) person will call an English speaking relative in another town (or state) to report an emergency. Second party calls are always the hardest to handle.
The time is not yet at hand to convert the emergency services to AI !

Steer/Drive by wire: These discussions are relevant to Risks as they are or will be implemented at some time. BUT! It is sort of the same as adding the computer to a small business; there are times that it is just not appropriate. Mechanical design considerations have been for some time at the

technological point to eliminate any of the problems (reasons) for such a computer system. Ask a race car driver what computer systems he wishes. Here the answer seems to be more emergency condition indicated than technologically capable. That driver wants a system to turn on the fire extinguishment system in .000001 second of the explosion or fire, and yet you will not see the air bag pop out of the MECHANICAL steering wheel. You have seen the severe crashes these people are exposed to, and yet they want the machine to be at hand, not computer. This will hold true unless the people start loosing to such a system, thus proving its merit.

Point 2. This is the, "eliminate the man" syndrome. If the speed and complexity of the systems are such so that a computer insertion to control it is necessary, then it is time to consider removal of the human element. This bridge is a hard one to cross. Project loss due to failure and the price of backup systems put the cost of such projects over the top. We still put the wo/man above price and yet when a multibillion dollar project is launched, the requirement of the human to be onboard is still paramount. Protection of the systems, uncalculated emergency procedures, patches and repairs incapable of the onboard systems are only feasible with the HANDS and brains of the crew, supported by their electronic and human counterparts in remote. Major system failure will cost not only the project, but also the crew. This possibly is the impetus for quality in design and manufacture. Do you work more carefully when there is a human life in the balance at the reception of your output? i.e., The program writer who discovered his program was inside the operating room during a heart transplant, and had a few thoughts about the possible bug.

Work ethics in the U.S.: Systems installation into the chain of mechanical elements is obviously an expected outgrowth of our technology. The desire to have modern systems replacing 100 year old mechanical ones runs back as far as the fellow that removed the square corners from the wheel. The real question is if the can opener really needs that keyboard input in conjunction with the clock card in order to do the job. If it is a desire of the customer to have such a system, so be it. System implementation seems more of, "Gee, look what I made. Where shall I put it?", than here is the problem, what shall we do to make it better.

Total redesign may be more appropriate than added-on systems. It is up to us to say enough is enough and initiate that type of improvement rather than amend a system.

>From: sigma!roman@entropy.ms.washington.edu (Bill Roman) >*RUMOR*
>I can't vouch for this personally... but a few years ago I spoke to a
>contractor who said he had been approached to write software for the
>Issaquah class ferries. [...] My friend refused the contract.

This type of reaction to an idiotic set of circumstances is of the highest quality. The only neglect here (not mentioned) was a blast to the authorities requesting the work.

It is a shame that in order to keep position in relation to other professionals, one must remain mute on problems such as this. I wonder how many lines of code be eliminated or dollars saved (redundant?) if there were a majority of professionals that acted in this manner?

Tell me, are the Risks that we are seeing more of a moral question or one of simple incompetence?

eww@oberon.lcs.mit.edu Wes Williams

Re: drive by wire

<dukeac.uucp!bet@mcnc.org>
Fri, 6 Mar 87 06:03:40 est

Representatives of GM recently gave a presentation here at Duke on the Chevrolet Corvette Indy. This "show concept car" (a one-of-a-kind) has about everything on it people have been worrying about in this forum; I went to the presentation and nagged the engineers about the points of concern that have been raised here. This car was built by Lotus Cars Ltd.; it might have been the project that started this discussion.

For starters, the term "drive-by-wire" is used in their glossies *not* to refer to the computer controlled steering, but to computer controlled throttle! The car is four-wheel-drive, with computer control over the split of torque between the front and rear wheels, designed to maintain maximum traction in all conditions of acceleration/deceleration. The "gas pedal" is connected to a sensor (and has a hydraulic ram behind it so the computer can simulate the feel of a mechanical linkage); the sensor concludes what acceleration the driver wants and delivers torque to the front and rear wheels. This is probably the most RISKy part of the whole car, in my humble opinion. It is a bit more comprehensive than the computer controlled idle adjustments and suchlike that are getting to be common these days.

It also has a computer controlled four wheel active suspension; when I asked them about the failure modes and potential RISKs in this subsystem, they replied that in the event of loss of power to the hydraulic system driving the active suspension, the coil spirings hold the car at its normal height above the wheels, and the hydraulic rams are designed to fail under loss of power into reasonable shocks. The ride would be mushy, but not dangerous (unless of course it failed in the bottom of a really tight turn). The computer controlling the system (1) has internal sanity checks throughout, and (2) has multiply redundant sensors; whenever any inconsistency is found in the system it fails into the powered down mode.

Finally, the computer controlled steering. The front wheels are normal manual rack-and-pinion steering; the front steering linkage has a sensor on it so that the computer can tell how far you have the front wheels deflected. Based on the deflection of the front wheels, the speed you are going, current acceleration vector, "weight" currently on each wheel, and suchlike, the computer deflects the rear wheels. In particular, at low speeds, the rear wheels turn the opposite direction from the front, tightening the turning radius substantially. At high speeds, they turn the same direction as the front wheels, making fast lane changes smoother; instead of slewing around, and rocking from side to side, the car tends to slip crabwise laterally. The total deflection available to the rear wheels in the prototype is 20 degrees

left or right of center; according to one of the engineers there they only would leave 5 degrees available in a production system (that's all that is needed). The system is once again equipped with multiple internal sanity tests, and dumps at the first sign of trouble; large springs center the rear wheels if the system dumps. In tests where they deliberately cause the critter to fail turned as sharply as possible, they found that at slow speeds the car could be stopped safely, and at high speeds the driver could keep control by steering the front to compensate (and proceeding slightly angled down the road). All in all, the severity of symptoms seem much less severe than a blowout; if the likelihood of such a failure can be reduced as low, then the steering shouldn't introduce too much RISK.

Bennett Todd, Duke User Services, Durham, NC 27706-7756; +1 919 684 3695
UUCP: ...{philabs,akgua,decvax,ihnp4}!mcnc!ecsvax!dukeac!bet
BITNET: DBTODD@TUCC

Autoland

Peter Ladkin <ladkin@kestrel.ARPA>
Fri, 6 Mar 87 13:03:07 pst

Those who do not like category IIIA autoland (auto up to main wheels on the ground, pilot has to lower the nosewheel) might avoid flying the Concorde, which uses it routinely at Kennedy and London Heathrow, and might also avoid flying in to London Heathrow, which I understand has Cat IIIA on all runways, used routinely in English Weather. It's been thoroughly tested in the field for many years.

peter ladkin

Re: Puget Sound Ferry Boats

Bjorn Freeman-Benson <bnfb@beaver.cs.washington.edu>
Fri, 6 Mar 87 07:56:53 PST

From a Puget Sounder who has followed the story in the papers...
The computers for the Issaquah class ferries were built by a private contractor to MP&E. This private contractor turned out to be a one man shop who did little or no quality control and went belly-up after the ferries were built. He/she did not leave any documentation behind.

The results were:

(a) The computers are poorly designed and built -- at one point the boards physically fell out of the card cage while under way.
(b) With no documentation, repair would be incredibly expensive.
(c) The failure of the computers (starting with the maiden voyage) had caused the public to mistrust them, and so replacement by a physical system is occurring.
(d) Many of the failures have been attributed to physical parts such as small relays. (i.e. The software said "slow down" but engine didn't.) A better overall system design would have helped.

Bjorn N. Freeman-Benson

Credit Card Limits

Clive Dawson <AI.CLIVE@MCC.COM>
Fri 6 Mar 87 15:12:47-CST

[This is another instance of an old problem, but worth rehearing.]

Yesterday I received a nasty letter from my credit union stating that I had exceeded my VISA card's authorized credit limit of $500 by $203. They advised me to pay up immediately or face the consequences, etc. etc. This was a bit of a surprise, considering that my credit limit was actually $2000.

The very next letter in my stack of mail contained the following:

> Dear Member:
>
> Please accept our apology for the recent letter stating you were over your credit line.
>
> We were attempting to implement a credit line increase into the system. Due to a programming error by our processor in Dallas, the old credit line was inadvertently removed and only the increase appeared on the account. Some members were declined on purchases due to this error.
>
> The new credit lines are now in the system and your account is in good standing. Your March statement will reflect the new credit line increase.
>
> We regret any inconvenience this may have caused you.
>
> Sincerely, [etc.]

I guess I was one of the lucky ones who didn't even notice the problem until I received both letters simultaneously. I would not have been at all amused had I learned of this on an out-of-town trip trying to rent a car or something.

Clive

NSA Monitored McFarlane House, Magazine Reports [A few new items]

Don Hopkins <don@brillig.umd.edu>
Fri, 6 Mar 87 13:07:58 EST

The government secretly monitored the home telephones of Robert C. McFarlane after he stepped down as President Reagan's national security advisor, according to an article in the Progressive magazine.

The magazine article said a National Security Agency electronic device was found in the sewing closet of McFarlane's home in Bethesda in January during a sweep ordered by his attorneys.

Spokesmen for the NSA and for McFarlane refused comment. The White House said it would have no comment until it saw the magazine, which is to be on newsstands Saturday.

The magazine quoted intelligence sources as saying that phone conversations of senior U.S. officials have been recorded for "archival purposes by the Pentagon and the CIA and for communication security by the NSA."

In the article entitled, "The White House Tapes, Again," the magazine quoted sources as saying the program produced "a still-undisclosed archive of recorded conversations" involving Reagan, Vice President Bush, former White House chief of staff Donald T. Regan and former National Security Council staff members Oliver L. North and John M. Poindexter.

The article, written by freelance reporter Allan Nairn, said McFarlane, who left the White House in December 1985, had been falsely told that a security unit on his home phone had been deactivated.

It said the unit uses a computerized encryption device that makes a call unintelligible to anyone trying to listen in without the proper equipment and authorized code.

The article said that the monitoring of top officials generally seems to have been done on a basis of express or implied consent and therefore would not appear to violate federal communications laws.

In McFarlane's case, however, the monitoring continued after he left the White House, the magazine said. A government team, according to the magazine, removed the unit's handset from McFarlane's home, but, unknown to McFarlane, left intact the system's control panel that enabled NSA to monitor calls, and in turn, record them.

After leaving the national security adviser's job, McFarlane continued to have access to classified material as unpaid consultant until the Iran-contra affair was disclosed in November. He took a secret trip to Tehran last May in a fruitless effort to free American hostages in Lebanon.

Search RISKS using swish-e

THE RISKS DIGEST

Forum on Risks to the Public in Computers and Related Systems

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

Volume 4: Issue 58

Sunday, 8 March 1987

Contents

The Sperry Plan, FAA Certification, and N-Version Programming

Nancy Leveson <nancy@ICSD.UCI.EDU>
07 Mar 87 10:34:16 PST (Sat)

Since my original message to Risks about the Sperry plan, I have visited the FAA Certification Office in Seattle and, for other reasons, the Boeing Commercial Aircraft Co. in Seattle. The Boeing employees I spoke to told me that they have rejected the Sperry plan for their software. However, it is planned to be used for a Category III autopilot for the MD-11. This autopilot is safety-critical for 30-45 seconds during autolanding. There is also great dependence on n-version programming for the fly-by-wire Airbus 320, but I have no details about the A320 software development such as the testing procedures used (except for a blurb in Aviation Week that states that n-version programming provides "optimum" protection against software errors in that aircraft).

To remind Risks readers, Sperry wants to use N-version software in place of "white box" (structural) testing. Black box (system) testing will still be performed. System testing would be done "back-to-back." Back-to-back testing means that multiple versions of the software are executed on the same test data. If they all agree on the answer, it is assumed that they are all correct.

Kevin Driscoll writes in Risks 4.55 that this plan is not really so scary. In order to follow the discussion, it is necessary to have some background on aircraft software certification.

There is a document used by the FAA (and written primarily by the manufacturers) called RTCA/DO-178A: Software Considerations in Airborne

Systems and Equipment Certification. It lays out the requirements for software development, testing, configuration control, and documentation. The requirements are pretty basic -- about what I would recommend for a good inventory program. In general the requirements are:

(1) developing software requirements and verifying them against system requirements [no requirement for any formality in the process];
(2) using a design discipline or method [not specified as to which one -- just says you need to use one] that makes software traceable, testable, maintainable, and understandable;
(3) doing a design review against requirements;
(4) using an implementation technique that is understandable, testable, and traceable to the design;
(5) doing requirements-based and structure-based tests including module testing, module integration testing, and hardware/software integration testing including a requirements coverage analysis and a software structural coverage analysis [this is what Sperry wants to eliminate except for system test]
(6) providing software configuration management;
(7) providing a quality assurance plan.

The document specifies software function criticality categories of:
Level 1 (flight-critical: failure prevents continued safe flight),
level 2 (flight essential: functions reduce capability of aircraft or ability of crew to cope with adverse conditions), and
level 3 (non-essential: failures could not significantly degrade aircraft capability or crew ability).

The difference in criticality level seems to determine what information is provided to the FAA for certification and, in some cases, which of the above requirements are enforced. For level 1 software, for example, the manufacturer must provide detailed information about the verification that was done. For level 2, in general only a summary description of the process along with a statement of compliance must be submitted. For level 3, no assurance is required. In terms of certification effectiveness, independent evaluation is possible only with information. So providing just a statement of compliance seems to me to imply that no external, independent evaluation is possible. There is no way to check that they actually did comply and that the verification that was done was adequate and correct. I certainly do not want to imply that the manufacturers and subcontractors will not try to do the best job possible -- after all, they have the liability and they are decent human beings who care about human life. The problem is that without external review we are depending on the competence of the people at these companies, and I am not as sanguine about the general state of software engineering knowledge and practice in industry as I am about the good intention of humans.

So far, though, things are not really TOO awful, but wait ...
The problem seems to arise from one sentence (which was added between version 178 and 178A and seems to be the major change) that states "Using appropriate design and/or implementation techniques and considerations, it may be possible to use a software level lower than the functional categorization." This is the kicker. Sperry is arguing

that although the software autopilot is Level 1, they are using n-version programming and therefore it can be treated as Level 2. There is also a phrase "the software level implies effort that ... may vary within criticality level." So they can modify any of the requirements also, it appears, within level (given that the FAA agrees).
BOTTOM LINE: even those very basic requirements that are specified above can be eliminated fairly easily. Personally, I would require MORE than is stated in DO-178A for both Level 1 *AND* Level 2 software development and verification.

As examples of what is possible, the DoD, besides requiring good software engineering practice, requires a safety and hazard analysis of the software. The Air Force and Navy also require an IV&V by a qualified company (Logicon does a lot of this) for all nuclear systems [called Nuclear Safety Cross Check Analysis by the Air Force and Software Nuclear Safety Analysis by the Navy]. These IV&V efforts are MUCH more rigorous than anything the FAA appears to be doing. Note that the DoD requires proof of the safety of the software itself and not just proof that the developers have satisfied minimal development practices.

The most amazing part of the RTCA document is the fact that using a particular method, such as n-version programming, can somehow magically change the criticality level of the software (from flight-critical to flight-essential or non-essential). Since the function of the software does not change with the development method, this appears ridiculous. I can only assume that they are arguing that the reliability will be so high that failures will never occur and therefore the criticality of the function is irrelevant; this is the only interpretation that makes sense to me. But there is no current software engineering technique that can guarantee such ultra-high reliability! (including N-version programming). And since they dismiss in the document the use of any measurement techniques (they state that currently available methods do not yield results in which confidence can be placed to the degree required) and don't even mention any formal verification methods, there is NO demonstration required that they have reached perfection (or any particular level of reliability) using the particular design or implementation technique.

In the Sperry case, their argument for N-version programming appears to rest on a simplistic model presented by Larry Yount at an AIAA Conference in Long Beach. This model assumes statistical independence between failures of the n versions. This assumption has been shown to not hold in controlled experiments and, in fact, is not believed by most researchers in the field. At a workshop this summer, Larry put up a chart that showed his model predicted 20,000 times improvement in reliability based on the use of n-version programming. Since actual experiments have found at best only 7-10 times improvement, his figures appear to be patently ridiculous.

Kevin Driscoll (Risks 4.55) states:

> In its letter to Sperry, the FAA says that this method "appears to be
> satisfactory" with the following constraints:
> a. Level 1 must be used for paragraphs 6.2.2 (Requirements Development
> and Verification) and 6.2.3 (Design).

> b. Formal configuration control must used and, if common errors are
> found, structural testing may be required for some or all of the
> modules.

Common errors have been found in EVERY experiment done so far in n-version programming (at least, in all that have checked for them which is about 4 or 5). The problem is that with only three versions of the software and the use of back-to-back testing, the only common errors that can be detected are those within only two modules. Any common errors found in all three of the modules cannot be detected (unless some outside method of correctness determination is used). In my experiment with John Knight at the University of Virginia, we found common failures in up to eight independently developed programs. Also, any errors that can be traced back to the specification will, of course, have a tendency to manifest themselves in common between the versions.

> c. Formal review and comparison of source code must be used to verify
> dissimilarity. Where this is not feasible, Level 1 structural test
> and analysis must be used.

How does one verify dissimilarity? In fact, how does one even define it? Obviously the programs must be similar in that they are computing the same function. The only dissimilarity we really want is a dissimilarity in failure behavior. Syntactic dissimilarity is irrelevant. Again, John Knight and I found programs that used completely different algorithms to compute a function yet failed on all the same input data. The problem is that certain input cases are inherently more difficult to handle. For example, when computing the angle determined by three points, programs tended to fail on inputs where the points were colinear or coincident. The errors were not the same nor were the algorithms, but they failed on the same input data. So looking to see that different algorithms are used is not adequate. This is the problem in talking about a concept like "dissimilarity" or "diversity" without ever formally defining it; there is no way to know whether you have it nor any way to measure it. It is similar to the problem with using the term "artificial intelligence" when the term "intelligence" remains undefined. One can merely claim that their program is intelligent and it is difficult to dispute it (or to prove it either). How does one prove or disprove that dissimilarity or diversity exists?

> It seems to me that c. is the same as doing structural analysis.
> Therefore, this method is not any less rigorous than "full" DO-178A
> Level 1.

I can see no relationship between verifying dissimilarity between two or three programs and structural analysis of the correctness of a single program; especially given that I know how to do the second but not the first. I am not quite sure what Kevin means by "less rigorous." Certainly, we have much more experience with structural testing than with n-version programming. There is no evidence anywhere that structural testing is equivalent to n-version programming (e.g., that they detect the same errors) nor that one can replace the other. Although somewhat beside the point, I would argue that even the *FULL* DO-178A is not nearly rigorous enough for safety-critical software.

> d. Functional tests of the system must be performed. It must be shown
> that the system will not have false alarms.

> However, how one complies with c. and d. I do not know.

THAT IS THE WHOLE POINT! Sperry is suggesting replacing something we know how to do with something nobody knows how to do and has never been shown to work with the degree of effectiveness required. I would certainly feel happier if the Sperry plan were tried first on real software that was not Level 1 or Level 2 (by real software, I do not mean just university or industrial experiments where the software is never used in a real production environment). I have few qualms about N-version programming being used in conjunction with normal software development techniques even on safety-critical software. But I have grave reservations about eliminating any testing or other standard procedures on the basis of using it. The problem, of course, is that developing multiple versions is expensive. So I assume Sperry is trying to cut down on testing in order to save money. Unfortunately, I do not know how to develop safety-critical software cheaply. For the most part, greater reliability and safety requires more money. Just using some sleight of hand to relabel the software as Level 2 or Level 3 instead of Level 1 does not make it any less safety-critical. And voting together relatively untested and unverified single versions has not been shown (in the experiments that have tried it) to guarantee high reliability or safety. In fact, the little experimental evidence available has shown that as the number of errors in the individual versions increases, the amount of reliability gain to be expected fron using n-version programming decreases.

I am still worried despite Kevin's attempt at reassurance.

Nancy Leveson, University of California, Irvine

Search RISKS using swish-e

THE RISKS DIGEST

Forum on Risks to the Public in Computers and Related Systems

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

Volume 4: Issue 59

Sunday, 8 March 1987

Contents

Safe software

Geraint Jones <geraint%sevax.prg.oxford.ac.uk@Cs.Ucl.AC.UK>
Sat, 7 Mar 87 00:41:38 GMT

IN RISKS 4:56, Hal Guthery makes the laudable plea that we component makers should take into account that some applications programmer will eventually want to make a `safe' system out of our components. He does not expect a painter to be responsible for the structural integrity of the bridge; he wants to be able to take that for granted. At risk of straining his metaphor, I would not expect the painter to complain at the architect's specifying rust-retarding paint for a steel bridge standing in salt water.

He suggests that modern parallel architectures (transputer systems) and languages (Ada, occam) are unsuitable, presumably less suitable than

others, for building safe systems: the assumption being that ``deterministic'' is a part of ``safe''. The fault with this argument is that often one does not require entirely deterministic behaviour from a system, and that constraining a design to be deterministic in every detail may make it harder to understand. The harder it is to understand something, the less likely one is to build it correctly.

Sadly, the real world out there beyond the interface chips is not particularly predictable in its behaviour, and does not take too kindly to being told to wait, and to do things just so and not in some other order. While the ``world'' is a part of one's system, one must be able to reason about non-deterministic systems. Would you really rather use a sequential programming language, and not be able to write some parts of the system (device drivers, interrupt routines, the Lord preserve us even operating system kernels) in the most natural and lucid notation?

If one is writing real-time programs, and there really is more than one thing going on at once, then it turns out to be very much easier to tell how long it will take to run a piece of code on the right multi-processor machine than when multiprogramming a uni-processor.

At risk of sounding like an INMOS salesman (usual disclaimers apply, not a penny do I get from them, more's the pity) they _do_ sell tools for measuring execution times, and in terms of the programmer's source code, not in terms of the execution times of instructions. Leave the instructions to the machine, it knows more about them than you do or ever wanted to. There _are_ hooks in languages like occam to make it possible to reason about the real-time performance of a program. (I would refer you in passing to a discussion in ``Programming in occam'', G.Jones, Prentice-Hall 1987, but you might think I had an ulterior motive :-)

The answer to questions like ``why can't I install my own scheduler?'' has surely to be that this is not a question that an applications programmer should know how to ask! In particular, if one is writing real-time programs, then the correctness of one's code had better not depend on how it is scheduled.

If we really want to build reduced risk systems, we should use those (intellectual and mechanical) tools which make it easiest to convince ourselves and others that we are making the right system. I counter the slur (that parallel means slippery) with the observation that you should not necessarily complain if your toolmaker offers you a nutcracker when you asked for a sledgehammer. There may be more moving parts in the nutcracker, it may require more dexterity to use, but the humble tool fitter thinks he has learnt something about eating nuts, and he may well not be entirely wrong.

gj

Computer Problem causes airline financial loss

Rob Horn <wanginst!infinet!rhorn@harvard.harvard.edu>

Fri, 6 Mar 87 11:30:31 est

From Wall Street Journal report of Florida Express CEO's statement:

> ``... computers in our own reservations office accurately displayed the availability of discount seats throughout our system, but the computers used by travel agents, who sell 65% of our tickets, erroneously indicated no availability of the cheaper fares on many of our flights.''

This apparently caused a significant drop in sales that may cause the airline to lose money this quarter. They indicate that the problem seems to have been solved but give no indication of what the nature of the computer problem was.

Rob Horn
UUCP: ...{decvax, seismo!harvard}!wanginst!infinet!rhorn
Snail: Infinet, 40 High St., North Andover, MA

Re: Altitude Encoders... expensive for some

Ronald J Wanttaja <ames!uw-beaver!ssc-vax!wanttaja@cad.Berkeley.EDU>
Thu, 5 Mar 87 09:52:32 pst

> From: jbrown@jplpub1.uucp (Jordan Brown)
> Subject: Re: Altitude encoders: $1500 for Mode C? No, $750.

I hate seeing notices like this, because of the fear that, a month from now, I'll hear Ted Koppel say "... The devices will cost aircraft owners $750..."

I suspect that the aircraft already had a transponder installed, and added an altitude encoder to it. And I'm all-fired certain that it had an electrical system.

For those not familiar with General Aviation, many aircraft do not have batteries or alternators. Ignition spark is provided by magnetos. The folks advocating mandatory altitude encoding transponders seem to forget that fact.

These aircraft are not that rare... at the airport where I kept my Cessna, I estimate that 5% did not have electrical systems. This airport is ten miles from Sea-Tac International. Let's see... $750 for the basic transponder, $750 for the altitude encoder, $2000 for an electrical system, 25 hours labor at $40/hr... $4500 upgrade cost for an airplane worth $6000.

Sure, and let's require everyone to install airbags in their older cars, too.

Relying on technology to solve a particular problem is nice, as long as you don't ignore real world conditions. Let the aviation community solve the problem, using its own expertise. There are too many self-appointed aviation safety experts out there, like Ann Landers, whose only qualification is that they fly on airliners a lot.

Ron Wanttaja (ssc-vax!wanttaja)

Influence of goal selection on safety

<pyramid!utzoo!henry@hplabs.HP.COM>
Fri, 6 Mar 87 20:51:46 pst

I've been reading the NTSB report on the Delta Tristar crash -- the one prominently featured in "Why Planes Crash" -- as it's been serialized in Aviation Week, and recently noticed something that hasn't received much attention that I'm aware of. After the Challenger disaster, it became clear that NASA was compromising safety because the goal of getting the flight rate up was inconsistent with taking all necessary time to ensure safety. The NTSB report pointed out something similar in the matter of airliners vs. windshear. Stripped of the aviation technospeak, one part of the report says essentially: "We are disturbed that most existing windshear-procedures training tells pilots that the ultimate goal is to continue the landing. We feel that once control is regained, the proper action is to abandon the landing and climb immediately to a safe altitude."

It seems to me that there is a significant general principle here: if safety is not part of the primary objectives, there will be a strong tendency to treat safety problems as temporary aberrations, rather than as indications of fundamental danger that may require abandoning the primary objectives.

Henry Spencer @ U of Toronto Zoology
{allegra,ihnp4,decvax,pyramid}!utzoo!henry

Re: Puget Sound Ferry Boats

Dennis Anderson <ames!uw-beaver!ssc-vax!dma@cad.Berkeley.EDU>
Wed, 4 Mar 87 15:18:19 pst

Here is a little more background about the ferry control problems. This may not be suitable for publication in mod.risks, but the USA Today article seems to have missed some important issues.

The problem is as much political as technical. A big part of the problem is that the State of Washington doesn't have schematics or software documentation for the control system. Under terms of the contract, those items are proprietary information and remain the property of the subcontractor that designed them. That subcontractor also went bankrupt and was bought out by Marine Power & Equipment.

As I understand it, it would be impossible to fix the computer systems without the design info.

Another failure mode: When loading and unloading, the ferry is held in its slip by running the engines at idle. The prop pitch control systems would occasionally shift into reverse pitch, causing the vessel to move away from the dock. One car went into the sound in one such incident.

Others have nearly done so.

I have ridden several of the Issaquah class ferries, and survived.

Dennis Anderson @ Boeing Aerospace ...uw-beaver!ssc-vax!dma

Re: Puget Sound Ferry Boats

<Frankston@MIT-MULTICS.ARPA>
Sat, 7 Mar 87 01:50 EST

How does one go about purchasing a computer control system for a ferry boat?

I keep looking for general significance in these failures and keep coming back to the social inertia inherent in adopting or adapting to a new technology. There is simply not yet an infrastructure that can fully manage computerization.

In general, I believe that in critical areas such as optimizing the behavior of wheels in a car or landing an airplane, the computer has a large advantage. The issue is not one of whether these system will and should be used. It is a question of when we will have enough understanding to apply these systems effectively with the proper engineering principles to deal with failure modes, intuitiveness of interface etc.

Re: Puget Sound Ferry Boats

<Frankston@MIT-MULTICS.ARPA>
Sat, 7 Mar 87 02:01 EST

In reading through the rest of the letters this week, I should amend my previous letter by noting that we don't really do a good job of engineering noncomputer systems. Bridges used to fall down 40% of the time until we learned to build them. I was told (but have not verified) that when building the Hancock building in Boston, the people spraying concrete (or whatever) over the riveted beams would often get ahead of the riveters and would not wait. The building is still standing, though did go through a period of plywood windows.

GOES satellites, Scotchbrite, Gnomic Maxims, and Mr. Bill

Martin Harriman <"SRUCAD::MARTIN%sc.intel.com"@RELAY.CS.NET>
Fri, 6 Mar 87 14:53 PDT

My vague memory is that the GOES satellites started failing prematurely because of an unauthorized change to a component; specifically, that a subcontractor changed the type of light bulb used in an optical encoder on a gyroscope. Someone with more spare time than I have could find this in Aviation Week and Space Technology.

Another major incident of this type was when, once upon a time, some helicopters started falling out of the sky (I believe they were large Sikorsky helicopters--my memory is getting vaguer by the second). This was somewhat upsetting (especially for those killed as a result)--the cause turned out to be an unauthorized (untested) change in a manufacturing step. The races for the main rotor bearing were supposed to be deburred with a wire brush; the bearing manufacturer switched to Scotchbrite pad, since it was easier to use, and seemed to produce the same results. The bearings started failing prematurely, and a number of unfortunate people (mostly in the North Sea oil fields) discovered how poorly helicopters fly when the main rotor bearing disintegrates.

Most of the contributors to RISKS seem much more frightened of software risks than mechanical risks (the steer-by-wire discussion is a case in point). Perhaps it's worth keeping in mind that mechanical systems have their problems, too: it's especially worth remembering if you are planning to use a mechanical system as the failsafe for some piece of software wizardry ("Oh, no, Mr. Bill: the emergency handwheel just came off in your hand! Watch out for the train... <crunch>").

--Martin Harriman martin%ucscb.ucsc.edu@ucbvax.berkeley.edu

[Deburred in the hand is worth 3 Bills in debrush. PGN]

Spreadsheet budget helping legislators

sewilco%meccts.mecc.com%ncar.csnet@RELAY.CS.NET <Scot E. Wilcoxon>
4 Mar 87 11:00:29 CST (Wed)

The Minnesota Legislature is now using a spreadsheet as an educational tool. Legislators can put their favorite proposals in the budget, but then have to find a way to pay for them.

The budget proposals made by Governor Rudy Perpich were used as a starting point. Dick Pfutzenreuter, staff director of the House Ways and Means Committee, took those proposals and added relationships and comments for many issues. When using the program a legislator may change budget amounts for any item, but then has to balance the budget or raise taxes. Items are labeled to remind users of the meaning of each number.

Pfutzenreuter says that about half of the House DFLers (non-USA readers: the DFL is a political organization) have used the program. The legislators have tended to spend more for their pet projects while avoiding cuts in education programs. He also says that each has tried many budget alterations, since it is so easy to do them on the spreadsheet. The Governor's staff has requested a copy of the program.

Technical notes: Pfutzenreuter got the Governor's proposals in Lotus format. He is using "The Smart Spreadsheet" by Innovative Software, which is able to read Lotus disks. Not all legislators have their own computers yet, but many legislators simply used the program in

Pfutzenreuter's office.

Scot E. Wilcoxon (guest account) {ihnp4,amdahl,dayton}!meccts!sewilco
(612)825-2607 sewilco@MECC.COM ihnp4!meccts!sewilco

[It will be interesting when someone breaks in and modifies the costing or even the wording of a bill, unbeknownst to the legislator... PGN]

Search RISKS using swish-e

Report problems with the web pages to the maintainer

Search RISKS using swish-e

THE RISKS DIGEST

Forum on Risks to the Public in Computers and Related Systems

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

Volume 4: Issue 60

Monday, 9 March 1987

Contents

Feel better now? [Risk probabilities in nuclear power]

I need a vacation <minow%thundr.DEC@decwrl.DEC.COM>
09-Mar-1987 1623

From a long article in the Boston Globe, Mar 9, 1987:

"When the owners of the Seabrook nuclear power plant recently proposed shrinking the plant's emergency evacuation zone from 10 miles to 1 mile, they based their argument on what may be the most comprehensive computer study ever done of a nuclear reactor.

"Engineers spent $4 million and 35 man-years of work assembling millions of bits of data on Seabrook's design, construction and maintenance, then plugged them into a huge main-frame computer programmed to simulate how the reactor would handle anything that could conceivably go wrong. What emerged was a 50-foot high computer printout analyzing 4.5 billion possible accident scenarios, from minor valve failures to catastrophic core meltdowns.

"A 4,700 page study concluded that with a one-mile evacuation zone, the risk each year of a member of the public's dying from an accident at Seabrook would be less than one in 10 million -- low enough, Seabrook's owners said, to justify a smaller zone. ...

"If the US Nuclear Regulatory Commission accepts that logic and the courts reject a likely legal challenge, the $4.5 billion reactor will be able to open despite [Mass.] Gov. Dukakis' refusal to participate in what he says is an unworkable evacuation plan. There are six Massachusetts communities inside the 10-mile zone, but none fall within the one-mile zone."

The article continues by discussing criticisms of the study, and "the little-understood field of probabilistic risk assessment."

Martin Minow minow%thundr.dec@decwrl.dec.com

Computers in the Arts (or The Show Must Go On ...)

<Jeannette.Wing@k.cs.cmu.edu>
Monday, 9 March 1987 10:39:47 EST

Over the weekend I attended a dance concert put on by a local college company here in Pittsburgh. It was announced before the show started that the computer that controlled the lighting was not working, but the show would go on. However, only stage lights would be used so that the audience would not get the intended effect and mood that color and spotlights could give. People were offered their money back--no one left.

I wonder what backup strategies are typically used for professional music, dance, and theatrical productions. For example, some people in the audience wondered why the lights could not just be done by hand. Do Broadway shows use backup computers just in case of failure?

> [There have already been two big losers -- "Grind" and "Les Miserables", reported in earlier RISKS issues. This is the old local-optimization false-economy problem. One can economize with cheap computer control systems, but if they crash on you, the overall cost may be quite high. I imagine there is some backup here. But, as you well know, there are many cases where the main system and the backup system both fail, or where it is the redundancy mechanisms themselves that fail! PGN]

Sensitive Intelligence Document Published On Magazine Cover

Stevan Milunovic <Milunovic@SRI-STRIPE.ARPA>
Thu 5 Mar 87 02:54:09-PST

[The following item is not directly computer related, but is illustrative of a kind of risk not previously noted here -- although I vaguely remember other cases in which sensitive VDT screen images have appeared in photographs. PGN]

Sensitive Intelligence Document Published On Magazine Cover

By CLYDE H. FARNSWORTH
c. 1987 N.Y. Times News Service

WASHINGTON - A picture on the cover of the current issue of The Foreign Service Journal shows a readable copy of one of the government's most sensitive intelligence documents, according to government officials. The Foreign Service Journal, published for members of the Foreign Service, is generally available to the public and has a circulation of 10,000. The document, a copy of the National Intelligence Daily, which is produced by the Central Intelligence Agency in traceable, numbered copies exclusively for the president and a small circle of others with top-secret clearance, was photographed on the desk of Ronald I. Spiers, the Under Secretary of State for Management. Spiers was the subject of the article referred to on the magazine's cover. The CIA intelligence summary, which reports the latest intelligence evaluations by the agency, was open to two pages, apparently about the situation in Lebanan.

A map of Lebanon was partly blocked by Spiers' left hand. He had some hand-written notes partly shielding the print on the facing page, but clearly visible at the bottom of the page was the number 121. Some text as well as codes, also at the bottom of the page, were not legible with normal magnifying equipment, but a Congressional aide with a background in intelligence said, ''Based on my time in the business, this is the kind of thing you could blow up and clarify what the final thing is with not even very sophisticated equipment.'' The aide continued, ''This is a major breach of security.'' An aide to Sen. Jesse Helms of North Carolina, the ranking Republican on the Senate Foreign Relations Committee, said, ''Anybody else in the government who did this would have been fired if this had happened to them.'' [...]

Mode-C Transponders (Re: RISKS 4.59)

Phil R. Karn <karn@faline.bellcore.com>
Mon, 9 Mar 87 15:57:34 est

As far as I'm concerned, people who fly on airliners only as passengers have every right to complain about general aviation aircraft without altitude-encoding transponders, since they seem to collide in mid-air with airliners with alarming frequency. I really get tired of this "I can do what I want with my neck, why is the government trying to tell me what's good for me?" routine.

The simple fact is that your actions put others (like me) under involuntary

risk, and preventing this sort of thing is the fundamental reason why laws and governments exist. I don't care whether 5% or 50% or 100% of small planes lack electrical systems; if they can't be flown without hazard to other planes, then they shouldn't be flown at all.

Phil

Physical risks and software risks

Eugene Miya <eugene@ames-nas.arpa>
Mon, 9 Mar 87 11:05:26 PST

I've been thinking about the nature of physical systems and the addition of software to them. The comments by Martin Harriman and the comments and bridges and buildings moved me.

I am reasonably familiar with Sikorsky helicopters, and it makes me wonder if we should should put information into software which takes long term degradation into a software system. It has some interesting consequences, and it would be difficult to think of all of them out before hand. Parnas points out that computers are basically discrete systems (obvious over-simplification), but real systems are less so.

Bio degradable software anyone?

--eugene miya, NASA Ames Research Center

Safe software

Scott E. Preece <preece%mycroft@gswd-vms.ARPA>
Mon, 9 Mar 87 08:36:49 CST

geraint%sevax.prg.oxford@Cs.Ucl.AC:
> The answer to questions like ``why can't I install my own scheduler?''
> has surely to be that this is not a question that an applications
> programmer should know how to ask! In particular, if one is writing
> real-time programs, then the correctness of one's code had better not
> depend on how it is scheduled.

Eh? The real-time code I've heard about has depended very strongly on tight control of scheduling -- cyclic scheduling of tasks and strong control of priorities and sequencing of tasks. Whether the people writing real-time systems are "application programmers" in the sense conventional in the US is another question...

scott preece, gould/csd - urbana, uucp: ihnp4!uiucdcs!ccvaxa!preece

---

Helicopter rotor failures

Peter Ladkin <ladkin@kestrel.ARAP>

Mon, 9 Mar 87 15:46:02 pst

As far as I remember, Martin Harriman is referring to the rotor failure on a Bristow Helicopters' Sikorky S76A in Scotland. The rotor hub has elastomeric bearings, which were wearing prematurely, and the bolt on the inside of the rotor shaft was taking shear as well as strain forces, whereas it was only designed for the latter. The inappropriate finishing technique to which Harriman refers was a contributory factor in the failure of the bearing under the shear loads. The wear was the main factor. I believe that the aircraft was also operating out-of-inspection, being ferried to a maintenance shop with an illegal passenger aboard. The only moral relevant to RISKS would be not to take a free ride in aircraft that are out of inspection.

Re: Electronic steering

D. V. W. James <vnend@ukecc.uky.edu>
9 Mar 87 20:00:52 GMT

>From: "Hien B. Tang" <hbt@ICSE.UCI.EDU>
>Side note: Isn't the F-16 a fly-by-wire plane? If electronic steering is
>safe, and reliable enough for combat jets, why wouldn't it be safe enough
>for everyday car?

Several reasons. Primarily due to the fact that while a combat jet is constantly maintained, your average car on the road is driven until something breaks and causes it to be undrivable before repair is even thought of. Also, there are a lot more cars of a given model on the road than there are a given aircraft in the air.

Second, your average F-16 pilot is well trained and knowledgable about his aircraft, as is his ground support (though less so than the pilot). Your average (American, though I have never seen any real evidence that other countries do a better job) automobile driver is barely aware of the way a car should be driven. How can it be otherwise? To get your lisense in the US all you have to do is prove you exist, answer a few questions, mostly about signs, and such, and then drive a total of at most a mile at low speed. The most harrowing part of the test for most people is the parking! But this may be irrelevant, what could the driver of an automobile do if s/he suddenly found out that they had no directional control? And what warning signs could they notice of impending (electronic) steering failure?

It certainly sounds like a nightmare to me...

cbosgd!ukma!ukecc!vnend; or vnend@engr.uky.edu; or vnend%ukecc.uucp@ukma.BITNET
Also: cn0001dj@ukcc.BITNET and Compuserve 73277,1513

Altitude Encoders... expensive for some

<LIN@XX.LCS.MIT.EDU>
Mon, 9 Mar 1987 22:36 EST

> ... There are too many self-appointed aviation safety experts out there, like Ann Landers, whose only qualification is that they fly on airliners a lot.

This is scary to me. The aviation community does NOT affect only itself. The "mere" qualification that someone flies alot is certainly good enough to give that person a legitimate interest in safety concerns. If a solution won't work, then it's up to you "real" experts to say why not, and to explain it in a way that others will understand it. Telling them to "stay out" just doesn't wash.

F-104 (Re: RISKS 4.56)

Elliott S. Frank <amdahl!esf00@Sun.COM>
Mon, 9 Mar 87 16:24:40 PST

The story referred to by munnari!csadfa.oz!davidp@seismo.CSS.GOV is an old one: it dates back (at least) to the early or mid sixties. [Aside: "The Choking Doberman, and other Urban Folklore" should be required reading for RISKS contributors.]

The F-104 suffered a spate of crashes when it was first adopted by the West German Air Force: the pilots thought that they were smarter than the terrain-following radar with which the planes were equipped. They were. However, the planes were faster than the pilot's reflexes. After a sufficient number of crashes, the cause was determined.

I also heard a similar story about early versions of the terrain-following radar on the F-111.

Elliott S Frank ...!{ihnp4,hplabs,amd,nsc}!amdahl!esf00 (408) 746-6384
[the above opinions are strictly mine, if anyone's.]

Search RISKS using swish-e

THE RISKS DIGEST

Forum on Risks to the Public in Computers and Related Systems

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

Volume 4: Issue 61

Tuesday, 10 March 1987

Contents

More on human errors

Brian Randell <brian%kelpie.newcastle.ac.uk@Cs.Ucl.AC.UK>
Mon, 9 Mar 87 15:53:22 gmt

Since my RISKS contribution on the BBC-TV documentary on human error, I have had a chance to find out somewhat more about some of the studies which have been made of human errors, and on proposals for improved system interfaces which would reduce the chance of human operator error. Some sample references which other RISKS readers who share my ignorance of this topic might find interesting:

J. Reason. Recurrent Errors in Process Environments: Some Implications for the Design of Intelligent Decision Support Systems. In "Intelligent Decision Support oi Process Environments" (ed. E. Hollnagel et al) NATO ASI Series, Vol F21, Springer Verlag (1986) 255-270.

D. A. Norman. Design Rules Based on Analyses of Human Error. Comm ACM 26,4 (April 1983) 254-258.

D. A. Norman. Steps Towards a Cognitive Engineering. Proc. Conf. on Human Factors in Computer Systems, Mar 15-17, 1982, Gaithersburg, MD.

Doubtless there are many other references, but I have not found any dealing with the analysis of faults within computer systems arising from errors made by their designer, which was my original hope. I checked with Jim Reason, who indicated to me that he does not know offhand of any such work. Incidentally, his paper listed above, and one entitled "The Cognitive Bases of Predictable Human Error" (Proc. Ann. Conf.of the Ergonomics Society, Swansea, UK, April 1987) used what I found a very interesting computer-like model of human cognition, in order to "explain" observed patterns of human error.

[Note that the entire April 1983 issue of CACM (which includes the first of the above Norman papers) is devoted to the humanization of computer system interfaces. PGN]

Re: Teflon flywheels and safe software (RISKS 4.56)

Brian Randell <brian%kelpie.newcastle.ac.uk@Cs.Ucl.AC.UK>
Mon, 9 Mar 87 10:12:43 gmt

The problems of building time-deterministic devices out of non-deterministic components was debated at length during a recent IFIP WG10.4 meeting, during a seminar on Hard Real-Time Systems, organised by Gerard Le Lann and Herman Kopetz. The view of a number of us was that "time determinacy" was an abstract concept, alright for abstract algorithms, but in general inappropriate for real systems - certainly not systems and devices whose components and/or design cannot be assumed to be absolutely faultless. Thus we preferred to regard all performance figures, even so-called "guarantees", as being probabilistic. Thus we viewed the task of the system designer as that of satisfying him/herself (and others!) of the probability of some given time constraint being exceeded remaining within some acceptable figure, rather than that of "obtaining determinism from non- determinism". Needless to say, even after the problem is recast in these terms, it will usually still be formidable!

Brian Randell - Computing Laboratory, University of Newcastle upon Tyne

ARPA : brian%cheviot.newcastle.ac.uk@cs.ucl.ac.uk
UUCP : <UK>!ukc!cheviot!brian JANET : brian@uk.ac.newcastle.cheviot

---

Re: Computers in the Arts (or The Show Must Go On ...)

Alan Wexelblat <wex@MCC.COM>
Tue, 10 Mar 87 10:52:08 CST

My wife is currently taking her MFA in lighting design, and I've run some of

the computerized boards -- so this is pretty much experience-based.

There are two kinds of "computerized" boards available today. One kind is designed with the computer built in; the other kind provides software and a black box (usually just a bunch of d-to-a converters) to connect some sort of PC (usually an Apple or IBM) to a pre-existing board.

In the first kind, you program light cues in advance. Each cue is a set of numbers (0-100) fed to dimmers. The numbers represent the percentage of maximum power fed through that dimmer. Then you load up the program and by pushing a single button, you move from cue to cue. Once a cue is in place ("hot"), you can change it by hand, but changing hot cues is usually only done in emergencies (like when a lamp blows out). The board software usually allows you to have a preset (the lights that are on while the audience is entering the theatre) and to preview the next cue in a sequence.

The PC-based software usually does the same thing but often has more sophisticated capability. Some programs will allow you to construct cue sequences on the fly by selecting out of a library of predesigned cues; others allow modification of the cue just before it becomes hot, etc.

Now, to answer your question: When the computer went down, the people in the booth could not access the sequence of cues (and probably didn't have a presetter on hand anyway). What probably happened was that the board operator set what's called a "standard wash" and left it. Basically, he (or she) didn't know what lights were supposed to come on when (stage managers call the cues by number, which doesn't tell you what lights are used for what cues).

This is an example of the RISK of not having paper copies of information that's on-line and of the RISK of not having personnel available to do the computer's job if it fails.

Alan Wexelblat
UUCP: {seismo, harvard, gatech, pyramid, &c.}!sally!im4u!milano!wex

---

Re: Computers in the Arts (or The Show Must Go On ...)

Jeffrey R Kell <JEFF%UTCVM.BITNET@wiscvm.wisc.edu>
Tue, 10 Mar 87 13:23:02 EST

In my spare time, I play synthesizer with a local band in a large showroom, and one of our techs here also works as stage hand in productions at the fine arts center. I have had exposure to the computer lighting systems... and seen one fail. The case you explained sounded a great deal like problems other than simply the computer. In all systems I have seen, all lighting controls can still be done manually (perhaps not as quickly, but you can use all the available lighting instruments). The computer simply digitizes the dimmer settings on the panel as it is programmed, and later replays them in real time. In either case, a real analog low-voltage signal goes down a real wire to the dimmer (power) packs at the stage area which control the lights. It would seem better to leave the settings digital and

multiplex them on a single cable to the stage, but I have yet to see this principle used (although it may in fact exist in a very large system).

The most RISKy component is the control cable leading to the dimmers themselves. If the computer goes bad, you still have manual control. If the cable goes out, gets broken, etc., you really have trouble. It is possible to turn lights off/on manually at the packs, but that would not be very feasible as a backup.

The new digital synthesizers are RISKy as well, speaking first-hand. I own a Korg DSS-1 Sampling keyboard (not an advertisement) which has 512K RAM and a 3.5 inch double-sided floppy for sample/program storage. When trying to change voices between songs during a stage black-out, I inadvertantly pressed 'system save' rather than 'system load' and, being in a hurry anyway (it takes 45 seconds to load), pressed the verification without looking. Out of personal stupidity, I had left the disk write-enabled. Realizing this, I attempted to abort the save, only to corrupt the directory of the disk (when it rains, it pours). Fortunately there was a backup disk (whew) but there was a considerable delay (several minutes is a lot of dead air during a concert).

I rather miss the days when your worst nightmare was having a note out of tune, or something relatively minor :-)

<Jeff>

Jeffrey R Kell, Dir Tech Services | Bell: (615)-755-4551
Admin Computing, 117 Hunter Hall |Bitnet: JEFF@UTCVM.BITNET
Univ of Tennessee at Chattanooga |Internet address below:
Chattanooga, TN 37403 |JEFF%UTCVM.BITNET@WISCVM.WISC.EDU

Local telephone service problems, serendipity, and synchronicity

<Jonathan_Thornburg%UBC.MAILNET@MIT-MULTICS.ARPA>
Tue, 10 Mar 87 00:42:26 PST

Around 11:30pm local time (PST) on 9 mar 87, our local phone system (area code 604, 736 exchange) died. Calls in progress were disconnected. After a minute or two of no dial tone, it came back up again. When the same thing happened again about 3 minutes later, I called the operator and was told "we've had a flurry of calls in the last couple of minutes". All seems to be ok now (an hour later).

The phone system in this exchange is an all-new digital one, installed with considerable fanfare about a year or so ago. I haven't heard any reports of other problems with it, and line quality for modem work has been excellent.

By a truly remarkable coincidence, at the time of the crash, I was scanning our on-line Risks forum archive file via a modem over the phone, and had read a couple of phone failure items only a few 10s of minutes previously.

It's interesting to consider what the odds are of having this sort of accident happen while you're reading about the chances and/or hazards

of this sort of thing. As it happens, they have been calculated by Luis Alvarez for a somewhat similar situation, reading about someone's death just after thinking of that person for the first time in a long time. He estimates of the order of 3000 such occurences per year in the US (this is an order of magnitude estimate only, with a *large* error margin). See

Science 148, 1541 (1965)

for details. Two followup items (in the context of the significance of such occurences to "parapsychology") are

Science 149, 910 (1965)
Science 150, 436 (1965)

- Jonathan Thornburg

[I recall seeing "China Syndrome" THE NIGHT BEFORE Three Mile Island. That certainly made an impression on me. However, seeing "WarGames" the night before reading about a big computer security scam was much less surprising. Considering that telephone system outages do occur (but don't tend to get national news coverage), I guess your tale is not all THAT surprising. The same goes for air traffic control outages -- see the next item. But there have been numerous reports of seemingly paranormal communications from people who have just died. (Who said RISKS is not eclectic?) PGN]

Computer Failure Delays Flights at Atlanta Airport

Peter G. Neumann <Neumann@CSL.SRI.COM>
Tue 10 Mar 87 14:13:37-PST

An ATC computer crashed yesterday, resulting in long delays in arriving and departing flights at Hartsfield Atlanta Intern'l Airport on 9 Mar 87. The main computer was down from 9:50 a.m. until 12:55 p.m. The backup system worked properly. However, it does not handle flight-plan information, which had to be done manually (and thus contributed to the delays). (FAA spokesman Jack Barker said, "Safety was never a problem.")

[There have been enough reports on the ATC system in RISKS lately that I am by no means including everything I find. But I wouldn't want you to think everything was perfect. And safety is never a problem unless it is a problem. Yogi Berra might have said that. PGN]

Ozone hole a false alarm?

<pyramid!utzoo!henry@hplabs.HP.COM>
Mon, 9 Mar 87 18:51:17 pst

A side note on the matter of skeptical software hiding the existence of the Antarctic ozone hole: the Jan 12 issue of Aviation Week notes that some doubts have been raised about whether the hole is real. The problem is that there was a lot of volcanic activity early in the decade, and the dust from it has been much more persistent at high altitude than anyone expected. The satellite instruments are not good at distinguishing dust effects from changes in gas composition.

Henry Spencer @ U of Toronto Zoology
{allegra,ihnp4,decvax,pyramid}!utzoo!henry

More on Requiring Mode C transponders

John Allred <jallred@labs-b.bbn.com>
Tue, 10 Mar 87 10:19:41 EST

> ... The simple fact is that your actions put others (like me) under
> involuntary risk, and preventing this sort of thing is the fundamental
> reason why laws and governments exist. Phil

Wrong, Phil. Pilot's actions place you at risk *only* if the pilots break the rules. In the case of several midairs between commercial and private aircraft, the "busting" of the Terminal Control Area by the private aircraft (intentionally or unintentionally) played a major role.

> I don't care whether 5% or 50% or 100% of small planes lack electrical
> systems; if they can't be flown without hazard to other planes, then
> they shouldn't be flown at all.

I could use this argument to justify any safety item *at any cost*. How about $30k for an active collision avoidance radar for a $6k aircraft? It would make things safer, wouldn't it? Clearly, there is a point of diminishing returns. The $1500 (or whatever) cost per aircraft for a mode C transponder could be better spend on training and enforcement.

John Allred, BBN Labs, Inc.

More on Requiring Mode C transponders

Ken Calvert <calvert@sally.utexas.edu>
Tue, 10 Mar 87 14:50:23 CST

>(karn@faline.bellcore.com:)
> The simple fact is that your actions put others (like me) under involuntary
> risk, ...

I have several problems with this, but the main thing is to point out out that it is clearly not the case that "small planes" without electrical systems and/or transponders can't be flown without threatening innocent airline passengers. I expect that most such planes virtually never enter the busy airspaces (i.e., Terminal Control Areas) where midairs tend to occur. One reason is that regulations ALREADY require radios and transponders for aircraft operating in TCAs, as well as permission from the controlling authority.

[These last two sentences reach an apparently false conclusion.
(For example, Los Angeles and Chicago routinely report many such
incursions each day.) There is a huge difference between regulations
and actualities -- which in general is often a problem system

designers tend to ignore! PGN]

Airplanes will occasionally collide, as will cars and trains. We should indeed be working to reduce the RISKs, but in many cases (and I think this is one of them) we should be focusing on the hard problem of making people better pilots (and drivers, and programmers), instead of throwing money and technology at the problem in order to appear to be doing something. Especially when (again, as in this case) there are probably also technical difficulties with the proposed "techological" solution (e.g., capacity of the ATC system).

[OK. Perhaps we have done enough on this for now. People are most often the weak link in ATC, but technology can help. However, if the people rely too much (or blindly) on the technology, then the existence of the technology may be debilitating. PGN]

Search RISKS using swish-e

THE RISKS DIGEST

Forum on Risks to the Public in Computers and Related Systems

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

Volume 4: Issue 62

Wednesday, 11 March 1987

Contents

"Software Safety: What, Why, and How"

Jim Horning <horning@src.DEC.COM>
Wed, 11 Mar 87 19:41:04 PST

Capsule Review of "Software Safety: What, Why, and How",
Nancy G. Leveson, ACM COMPUTING SURVEYS, Vol. 18, No. 2

"This survey attempts to explain why there is a problem, what the problem is, and what is known about how to solve it. Since this is a relatively new software research area, emphasis is placed on delineating the outstanding issues and research topics." [From the Abstract]

I've often wished that there was a good survey of the RISKS field that I could recommend to people who weren't as well informed on the subject as I thought they ought to be. I'm pleased to report that such a survey has now been published in a widely accessible journal by a frequent RISKS contributor. Software safety is the central theme, but many other aspects of risks to the public in computer systems are mentioned. ("Mishaps are almost always caused by multiple factors, and the relative contribution of each factor is usually not clear.")

Regular readers of RISKS will find much of the material familiar. But they should appreciate the careful documentation of numerous software-related mishaps and the perspective obtained by pulling back a little from our daily batch of anecdotes and looking for general issues and principles. The paper is well organized, and lucidly written. More than 100 references point interested readers to more detailed and/or authoritative information. There is also a general bibliography with 28 entries.

Despite the title, this paper doesn't tell how to produce absolutely safe software. Instead, it tells how hard it is, and why it is hard. Activist readers of RISKS will probably feel that it stops just short of some obvious conclusions and calls for needed action. (However, I'm sure that it would not be possible to get a consensus of this group about what the "obvious" conclusions and actions are.)

(This issue is dated June 1986, but my copy arrived last week. That this is a Publishing Risk, rather than a Postal Risk, is indicated by an apology printed at the front of the issue.)

Jim H.

> [Nancy herself proposed a solution to the last-mentioned problem -- simply declare the June 1986 issue to be a special combined issue dated June/ September/ December 1986/ March 1987. However, subscribers might feel cheated. PGN]

Beef with Restaurant's Hi-Tech Computer

<arens%arens3b2.uucp@usc-cse.usc.edu>
Wed, 11 Mar 87 12:58:17 pst

This happened to me several months ago, but I only just realized that it might be of interest to this group. My wife and daughter and I went to a rather fancy restaurant here in LA. We all ordered steak-type dishes and specified various degrees of doneness, all on the rare side. As we were eating our first courses there was a short blackout, lasting approximately two minutes. The restaurant remained illuminated by the candles on the tables.

When the main courses came they were very overdone. Our waiter took a peek at the food and then called the manager. The manager apologized profusely and blamed the computer that controlled the kitchen(!). As far as I could figure out, he was claiming that the blackout wiped out the memory of a computer which (among other things?) controls cooking times. When the power returned, the chefs had to try and recall how

long things had been cooking, and some mistakes occurred.

I have no idea if this was the truth or whether the manager simply thought that a high-tech excuse would be most effective.

Since we were too hungry to wait for new dishes, we ate what we had received anyway. We were not charged for the meal.

Yigal Arens arens@usc-cse.usc.edu

[This does indeed suggest a completely new line of high-tech excuses. PGN]

Electronic Steering

<mlbrown@nswc-wo.ARPA>
Wed, 11 Mar 87 09:27:29 est

I haven't had the opportunity to follow all of the discussion on the electronic steering issues that have been in the Risks Forum. I notice that there seem to be two sides: those who are scared and those who believe that the manufacturers will develop a safe product. Look back at several of those things that manufacturers should have caught: Pinto gas tanks, Audi 5000's sudden acceleration, Ford E-350 ambulances and their propensity to catch on fire. There are thousands of examples of such potentially catastrophic hazards that have made it through the design and development into manufacturing. Every car manufacturer has had problems of this nature. Yet, the tools and techniques for safety analysis of hardware have been around for many years. They can be very effective if properly applied. Yet we still have problems cropping up. Now we are proposing to allow steering to be controlled by software, control systems for which we do not have the tools and techniques that exist for hardware systems. Every software engineer will tell you that it is impossible to eliminate all of the defects in software: therefore, we have to ensure that the defects that remain do not cause a safety problem. Not a simple task. The process has to start at the concept stage. The software requirements must take into consideration the failure modes that can occur and develop traps to ensure that the system fails safe. The implementation of the safety requirements in the software requirements must be thoroughly analyzed and tested. Even then, it is difficult to develop a "warm, fuzzy feeling" about this system. Years of development can be destroyed by a simple failure that results in a fatal accident.

Mike Brown, Chairman, Triservice Software Systems, Safety Working Group

Enhanced 911 risks

<mlbrown@nswc-wo.ARPA>
Wed, 11 Mar 87 09:13:27 est

Several people have commented recently about errors in enhanced 911 systems that resulted in misdirecting police, fire or rescue personnel. In these

instances, a big safety issue is present. In my capacity as Emergency Services Coordinator for my county, I have been involved in investigating an enhanced 911 system for us. The system that has been proposed offers the dispatchers the capability of entering information in addition to the physical location of a caller into a master database. This database is located quite some distance from our locale and services a number of jurisdictions. Suggestions that have been made by our fire and rescue personnel include inserting information such as handicaps or special medical problems of residents, special problems that may be encountered in gaining access to people (e.g., having to ford a stream), etc. As the "good ideas" expanded, it was suggested that people who may have toxic materials (farmers with farm chemicals) or other hazardous materials (we have a number of gun clubs that store black powder or reload their own ammunition), gun collectors or others who may have valuables in their home, etc. be included in this database. Immediately I had visions of someone misusing the database to commit crimes, etc. How do we ensure the security of a database of this nature when the people who are required to have access to it cannot be trusted? Recently, two local jurisdictions have had sheriff's deputies arrested for participating in a burglary ring that has been functioning in the area for 15 years. Scary, isn't it? And then there's Big Brother....

Mike Brown

[Maybe that is the same gang that was rampant in New Jersey in the 1960s, giving free estimates on police-linked burglar alarm systems, after detailed on-premise inspections , with the more profitable houses being burgled if they did NOT subscribe. PGN]

Computers in the arts [Manual vs computerized lighting systems]

<dmc%videovax.tek.com@RELAY.CS.NET>
Wed, 11 Mar 87 02:07:37 PST

In my youth I worked as a stage manager and lighting designer/operator for a number of summer stock (and winter broth) companies. The most complex show we ever pulled off had about 300 cues over a two hour period. (I do think the art suffered as a result.) This was on pre-computer but modern (1966) equipment, with 72 x 6 KiloWatt electronic dimmer channels, and 4 presets (four slider pots per channel). The control room contained a desk with master controls, and a side-wing with 288 slider pots on it. On our 300 cue show, we had 3 people operating...

When I later worked for the Canadian Broadcasting Corporation in Montreal (1972), the lighting system for Studio 42, a 600 seat auditorium, had 600 12 KiloWatt channels (one per seat :-). The channels were connected via a 48 volt patch panel to 80 control levels. The patch panel was a 600 by 80 matrix wherein the operator inserted a pin to make a connection. (Multiple assignments picked the lowest numbered control level). The 80 control levels had a primitive computer system for storage/recall, but the one slider pot on the control desk could be driven to the level of a recalled channel by a motor, and would detect the operator's touch (capacitively) to permit the setting of levels.

Neither of these systems ever had all channels working at the same time. The electronic dimmers were packaged in racks and racks of drawers, and it was a simple matter to repair a vital channel by moving a drawer. The 1966 vintage Strand Electric console had sufficient internal parallelism that we lost channels and pots, but never the whole thing. (I vaguely recall a dual power supply). The CBC system was another story, and a fully qualified Group 8 (the top pay scale) NABET technician was always in the building when Studio 42 was in use. The lighting system failed occasionally, but never took more than an hour or so to restore to operation, since we stocked a full board replacement inventory. In my five years there it never failed on air.

I see current lighting control systems at the television trade shows. They use multiplexed twisted pair to connect a small control desk to `intelligent' dimmer boards. Smaller systems build the dimmers right in. The control desk contains a microprocessor that operates each channel, and reads levels from a floppy disc. The key to making these systems redundant is buying two control desks. Individual dimmer channels can fail, but that won't shut down a show.

The amount of rehearsal needed to choreograph the operation of a manual lighting console is significant. A failure of the modern control desks means the system is down, since there aren't manual controls any more. (It's usually possible to wire a channel on.) The technical solution is simple (buy or rent another control desk for performances) but the people making these decisions are often not technical (trust me), and view such backup as a luxury.

Don Craig, Tektronix Television Systems

Computers in the arts -- The Show Must Go On.

Glenn Trewitt <trewitt@amadeus.stanford.edu>
11 Mar 1987 1113-PST (Wednesday)

One of the most painful memories that I have:

Last fall, I attended a Pilobolus modern dance performance at Berlekey. Their last segment was a performance of "Carmina Burana", accompanied by a compact disk. This is a long piece, perhaps 20 minutes. About two-thirds of the way through, when the performers were dancing "blind" (they had various things on their heads), the disk skipped to a different section. Many people didn't notice this, but I had seen the performance before and listened to the music at home. The performers were REAL good -- they recovered perfectly and the show went on.

[What an ORFFul experience! PGN]

For about 2 minutes more, that is. At that point, the disk went nuts and started playing random 10-second bits of music. Generally, just enough for the performers to start to recover. This went on for about a minute before they gave up and turned off the "music". But it seemed like an eternity, with the poor dancers up there on stage, just thrashing.

I see the risks here as different from other risks associated with any other pre-recorded music, because almost all other failures are not so catastrophic. With a record, for example, you can just nudge the needle and continue. On the flip side, it occurred to me that it was quite possible that someone in the audience had, with them, the technology to fix the problem. Namely, a portable CD player, perhaps with the same CD. An amusing thought.

- Glenn Trewitt

[Although off the subject of RISKS, this is of course a common failure mode of CDs -- not just a skip and a jump, but wildly erratic behavior. Similar things happen in digital computer control systems (as opposed to analog) -- slight errors may translate into wildly erratic behavior, e.g., a wild control transfer... PGN]

Mode C

Ken Calvert <calvert@sally.utexas.edu>
Wed, 11 Mar 87 09:41:53 CST

[Me on Karn on mode C for all:] (RISKS 4.61)

> ... I expect that most such planes virtually never enter the busy airspaces
> (i.e., Terminal Control Areas) where midairs tend to occur. One reason
> is that regulations ALREADY require radios and transponders for aircraft
> operating in TCAs, as well as permission from the controlling authority.
>
> [These last two sentences reach an apparently false conclusion.
> (For example, Los Angeles and Chicago routinely report many such
> incursions each day.)

I don't see how my conclusion is false. My conclusion was NOT that incursions do not occur. The point is that an Airplane Without A Transponder is not a greater threat to other aircraft IF it never goes in airspace where a transponder does any good (busy terminal airspace or airways). Moreover, I have not seen anything to indicate that all or even most incursions into TCAs are made by Airplanes Without Transponders. Have you?

[Absolutely. There seems to be lots of evidence that the incursions are by dingbat pilots, generally without appropriate avionics (adequate, nondefective, ...). In the Aeromexico case, the controller was totally distracted by dealing with one dingbat, and ignored another -- BOTH of whom were transgressing. PGN]

In my understanding (as a temporarily inactive Private Pilot) the only thing that requiring Mode C on all aircraft does that the current regulations don't is require Mode C on aircraft NOT operating in busy airspace. If the current regulations don't work, this won't either. As you noted, there's a difference between regulation and reality. Transponders have to be turned on to work. Clearly some TCA incursions

are made by planes with Mode C transponders - irresponsible/incompetent pilots may fly all kinds of airplanes.

On the other hand, if the proposal is to have all aircraft equipped with Mode C that operates AT ALL TIMES, then the proposal must also require ATC to monitor all aircraft. As others have noted, I think it will be some time before the system can handle that, although that may be a worthy goal. Even then, incursions will occur. And your comment applies here:

>...rely too much (or blindly) on the technology, then the existence of the
> technology may be debilitating. PGN]

As a side note, my brother has been training to become an Air Traffic Controller for about nine months. He won't even sit down at a radar screen for a long time yet. New controllers must be completely familiar with the "old" manual system, which is of course used when things break down (actually it is always used; radar and computers are simply an aid). My impression from speaking with him is that the ATC system has a healthy distrust of (at least some kinds of) technology.

Ken Calvert, Univ. of Texas Computer Sciences

Re: Plane Crashes (RISKS 4.56)

Ronald J Wanttaja <ucbcad!ames!ll-xn!ames!uw-beaver!ssc-vax!wanttaja@ucbvax.Berkeley.EDU>
Wed, 11 Mar 87 08:49:52 pst

> In Europe there was a spate of (F-111?) crashes. The apparent cause of
> these crashes was pilots (1) believing they could fly the plane on their
> own without the help of any dumb computer, (2) turning the computer off,
> and (3) promptly flying into a mountain.
> Any Hints? DavidP

Don't know much about this particular case, but there is a famous story about the early days of the F-111 in Southeast Asia...

The F-111 was the first fighter-bomber with Terrain Following Radar. The radar controlled the plane through the autopilot to "hug" the earth; flying about 200 feet above ground level. It would look far enough ahead, and if an obstruction was sighted, the plane would pull up at the appropriate moment at a pre-programed G level (for those interested in further details of this type of flying, see the archives for rec.aviation).

The first combat crews were trained in the US, then send to Thailand to fly missions to North Vietnam. They had a high loss rate for night TFR missions. Then they found out why:

The TFR was set to fly the plane at 200 feet. The TFR couldn't see trees, and some trees in SE Asia grow over 250 feet high...

Ron Wanttaja (ssc-vax!wanttaja)

Re: Results of a recent security review (RISKS 4.52)

"Arnold D. Robbins {EUCC}" <arnold@emory.arpa>
Wed, 11 Mar 87 12:59:30 EST

In article Risks 4.52 Andre Klossner writes on the licensing of OWNDIR.
> [... and will someone sue AT&T if, after a license is duly obtained, a
> devastating Trojan horse is perpetrated using this flaw/feature ? PGN]

There has been a bunch of discussion about this in mod.os.minix; basically within a year of the patent, it was released for Public Use, i.e. anyone who wants to can use the setuid concept (which is why minix does). The article there cited real U.S. Patent Office publications giving the details. (I probably should have saved the article but didn't.) Anyway, I'm writing to try and cut off the spread of misinformation as early as possible.

I find the moderator's point more interesting; the people to sue would be the manufacturer who incorporated the feature, not AT&T who invented it...

Arnold Robbins
CSNET: arnold@emory BITNET: arnold@emoryu1
ARPA: arnold%emory.csnet@csnet-relay.arpa
UUCP: { akgua, decvax, gatech, sb1, sb6, sunatl }!emory!arnold

Risks of Maintaining RISKS

Peter G. Neumann <Neumann@CSL.SRI.COM>
Wed 11 Mar 87 11:56:14-PST

I received a complaint from Dave Parnas that he was suddenly receiving mail intended for the automatic BITNET mail list maintainer. It turns out that two readers forgot, or did not read, the old instructions. Sorry, there is nothing I can do on BITNET to prevent it, although I make a big effort (but still not foolproof) on CSL.SRI.COM. (At least it hasn't happened here yet, although I have received numerous retries to RISKS following rejected mail inappropriately sent to the LIST.) PLEASE READ THE MASTHEAD. Reminder for BITNETters, once again:

For WISCVM, send mail to LISTSERV@CMUCCVMA, with a single line request:
SUBSCRIBE MD4H your name or UNSUBSCRIBE MD4H your name
For FINHUTC, send mail to LISTSERV@FINHUTC, with a single line request:
SUBSCRIBE RISKS your name or UNSUBSCRIBE RISKS your name
For UGA, send mail to LISTSERV@UGA, with a single line request:
SUBSCRIBE RISKS your name or UNSUBSCRIBE RISKS your name

(All three may be work interchangeably -- I'm not sure.)

Search RISKS using swish-e

Report problems with the web pages to the maintainer

Search RISKS using swish-e

THE RISKS DIGEST

Forum on Risks to the Public in Computers and Related Systems

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

Volume 4: Issue 63

Thursday, 12 March 1987

Contents

Re: Teflon flywheels and safe software (RISKS 4.56)

<mok@saucer.cs.utexas.edu>
Wed, 11 Mar 87 19:32:34 CST

[Response to comments of G. Jones and B. Randell:]

It is a truism that we, as engineers can only hope to minimize the probability of failure in the systems we build (assuming that you believe in quantum mechanics). The relevant question is of course how to build systems in such a way that we can have as much confidence as possible that they will meet specifications with reasonable resources. To build a system which has

critical timing constraints, we can allocate resources carefully so as to enable us to prove that the system will invariably meet the specified timing constraints, ASSUMING that the hardware functions correctly and the external environment does not stress the system beyond what it is designed to handle. The fact that the hardware may not function correctly or that the operating conditions imposed by the external world may exceed the design limits with a certain probability DOES NOT absolve us of the responsibility to try to allocate resources carefully so as to invariably meet the critical timing constraints. Yes, performance figures are ultimately probabilistic. But if a real-time software designer can at all help it, the source of uncertainty should not be due to the adoption of a resource allocation strategy which is outside the control of (worse still, not understood by) the software designer. I do not want my real-time program to cause a plane to crash or an oil-drill platform to topple over in rough seas just because I cannot predict that a tight loop takes twice as much time to run when the processor decides to flush its data cache at an inopportune moment! I think this type of predictability is the "time determinancy" that Scott Guthery was referring to in his message. It has nothing to do with sequential programming. It is a property that I certainly prefer to see in a safety-critical system. I suspect you would too.

There are many interesting and important research problems involved in designing predictable real-time systems, i.e., guaranteed to meet certain behavioral and timing specifications. Sometimes, the implementation language can get in the way, e.g., see [Volz and Mudge 86], [Mok 84]. Having a multi-processor system does not necessarily make it very much easier to meet timing constraints. Even if you have one processor for each process, you still have to make sure that the communication subsystem can deliver all the time-critical messages. This communication problem is likely to be harder to solve the more processors you employ. (Formulated properly as a combinatorial optimization problem, a variety of this communication problem can be shown to be NP-hard, but that does NOT mean that practical solutions do not exist.) On the practical side, there are always the engineering tradeoffs that need to be researched, e.g., should we use as few processors as possible to meet the specifications so that we can have as many extra ones around to replace ones that fail on-line? If we use one processor for each process, will the power supply generate so much heat that the avionics becomes less reliable because of higher operating temperature? If I am writing a really tight timing loop (talking about microseconds, not milliseconds), does it suffice to be able to measure execution time in terms of the programmer's source code in a high level language? And how do I find out how the on-processor instruction/data cache affects execution timing, if I am allowed to measure execution time only at the high level language level? There are also many other issues which are more theoretical in nature, especially about the part the scheduler plays in satisfying behavioral/timing specifications (more about this later?). All these need to be studied carefully so that we can design real-time embedded systems that the public can trust.

-- Al Mok

[Volz and Mudge 86] "Instruction Level Mechanisms for Accurate Real-Time Task Scheduling", Proceedings of the IEEE Real-Time Systems Symposium, pp. 209-217, New Orleans, Dec 2-4, 1986.

[Mok 84] "The Design of Real-Time Programming Systems Based on Process Models", Proceedings of the IEEE Real-Time Systems Symposium, pp. 5-17, Austin, Dec 4-6, 1984.

Re: Electronic Steering (RISKS 4.62)

Bob Ayers <ayers@src.DEC.COM>
Thu, 12 Mar 87 09:47:04 pst

In Risks 4.62, mlbrown@nswc-wo cites several "things that manufacturers should have caught" and mentions three, namely "Pinto gas tanks, Audi 5000's sudden acceleration, Ford E-350 ambulances."

Now from previous postings on Risks and elsewhere, it is clear to the non-hysterical that there is no "Audi 5000's sudden acceleration" except for that produced by the driver stomping on the accelerator. (Experiments where both the brake and accelerator were floored disprove the 60-Minutes docu-drama theories.) (And, to forestall weak replies that the "thing that should have been caught" was only the pedal layout, I'll remark that I've seen it stated and not denied that the Audi's pedal layout, while skewed, is by no means the most skewed layout on the market.)

The perceptions about Pinto gas tanks, too, are largely the result of public alarm (I might say hysteria), fanned by those in charge of selling newspapers. In actual government crash-tests, the Pinto
a) passed the government-defined government-given tests and
b) was not even at the bottom end of the vehicles that passed.

I haven't heard of the "Ford E-350 ambulances and their propensity to catch on fire."

Inputs For Quantitative Risk Assessment

<"guthery%asc%slb-doll.csnet@relay.cs.net">
Thu, 12 Mar 87 09:52 EDT

While I realize that a totally time-deterministic system is unachieveable (on quantum theoretical grounds if none other) I am unwilling to simply throw up my hands and hack code until everything seems to work correctly.

My definition of a real-time system is a system in which time is a quantitatively managed resource. The key word here is QUANTITATIVELY. Scheduling is obviously the very heart of time management. Not only am I repulsed by the notion that people are to be told that there are questions that they may not ask, the correctness of a real-time program depends first and foremost on how it is scheduled. Telling a real-time programmer not to care about scheduling is like telling a scientific programmer not to care about units.

In doing quantitative time engineering, I am prepared to work with tolerances and with probabilities. If I'm working in microseconds,

I can do my calculations with some nanosecond slop. I can also carry out my calculations with probability distributions rather than values. But I want to be able to make statements like the following at the end:

> "The time between when you start to depress the brake pedal with velocity v until the brake shoe makes contact with the drum is k milliseconds plus or minus j microseconds."

or

> "After you start depressing the brake pedal with velocity v the brake shoe makes contact with the brake drum in at least m milliseconds with probability n."

In other words, I want to provide my customers with the same sort of quantitative risk assessment information that the people who build medical systems (drugs, procedures, treatments, therapies, etc.) are required to provide their customers.

In the work that I do, the execution time of one instruction counts. For some of the machines I'd like to work with I am unable to obtain either tolerance-bounded or probabilistic measures of instruction execution times. I had an opportunity to chat with the designer of the Transputer recently. Not only did he not know the execution time distribution the instructions, he didn't really care what they were. This is not a directed criticism. All of the advanced system designers I've spoken with (processor, language, operating system, network, etc.) abandon time determinism at the drop of a hat. It's the in thing to do.

What I'm making a pitch for is quantitative risk assessment because with it will come quantitative system engineering including quantatitive time engineering. We all praise safe systems and deride unsafe ones but this is just Monday morning quarterbacking. The question is how do you build a safe one and avoid building an unsafe one. The scientific method seems to have worked well in other sciences, maybe it's time we gave it a whirl. Or maybe we just having too much fun playing in the silicon.

Re: Active car suspension

Geof Cooper <imagen!apolling!geof@decwrl.DEC.COM>
Thu, 12 Mar 87 11:05:17 pst

The French auto manufacturer, Citroen, has been selling cars with active hydraulic suspension since the advent of the DS series in the late 50's. It probably used an analog computer, which is a little off the topic here, but the benefits and risks might be of interest to people considering suspension controlled by digital computer.

The suspension compensates to give better traction when going around corners, down or up hills. It does this by actively tilting the car closer to upright. The car rides high at city speeds for better clearance of bumps and gets closer to the rode the faster you go, for better highway stability. You can also flip a lever in the cab and have the car rise a foot off the ground to go over snow, on dirt roads, etc.. It gets higher than a jeep.

The hydraulic system replaces the conventional car jack. To change a tire, you raise the car to its highest position, put something akin to a jack stand underneath the middle of one side, and lower the car again. The flat tire rises into the air (RISKs: doesn't work right if you're on a hill, you need someone to sit on the car if you are just trying to rotate tires).

The same facility allows the car to drive on straight roads with only three wheels. Thus, a flat doesn't cause you to swerve, and a blowout doesn't cause you to go out of control (RISK: my father once drove for five miles on a flat because he didn't know anything had happened).

As you might imagine, driving in a Citroen 15-20 years ago was a bit like driving in a concept car. And the suspension is only one of the advanced features it had.

There are some interesting RISKs. The car "settles down" after you turn off the engine. Since in city-mode it runs higher than most cars, you could end up settling down on someone else's bumper. The hydraulics will not lift the car up in that case. If you forget that you have the suspension in the raised position and go on the highway, the car is not as stable as it would otherwise be.

My father once had a break in the rubber tubes carrying hydraulic fluid while on the highway. All the warning lights in the car went on at once, including a large red light that said "STOP". The car remained stable, but he lost power brakes, power steering, and power suspension all at once, and had to get towed away. A normal precaution was to carry an extra can of hydraulic fluid around with you.

- Geof

Phone: (408) 986-9400 (work)
Postal-Address: IMAGEN, 2650 San Thomas Expressway, Santa Clara, CA 95052

Ozone hole a false alarm? (Response to Henry Spencer, RISKS-4.61)

Mark Brader <mnetor!msb@sq.com>
Thu, 12 Mar 87 14:07:13 EST

Scientists studying the problem from Antarctica announced some results that were covered by TV news recently. They said that products such as chlorine dioxide were found at 50 times the expected levels, which indicates that the ozone really is combining with chlorofluorocarbons and the need for action is urgent. I don't know how the measurements were made, but they seemed convinced.

Mark Brader

[This is getting a bit peripheral to Risks, but I don't think in view of the above that it's right to close the topic with the note from Henry, who, incidentally, has no TV. - msb]

[[It is still relevant: there is still a problem if the computer model is incomplete. But, I tend to put messages of lesser relevance

or lesser general interest toward the end of the issue. PGN]]

Phone problems (RISKs in auto-dialers)

David Barto <scubed!megatek!barto@seismo.CSS.GOV>
12 Mar 87 10:43:16 PST (Thu)

Recently here at Megatek, we have had a couple of problems with our phone systems. Both are the fault of the operator NOT checking that the information typed in was correct. The first was mine, the second someone else.

My mistake was in reversing 2 digits in the phone number. Instead of calling a computer, I called a person. Every hour, for 4 days. The person complained to the phone company who traced it to us. I did not notice since I had 2 phone numbers to try, the first failed and the second worked. I thus ignored the problem, went to USENIX, and while I was gone the problem was reported. (See what you get for making changes on a friday before going on a trip? :-)

The second was more serious. To call a long distance number the prefix was 1-919-XXX-XXXX, the person entering the number entered 91, followed by 2 backspaces to enter the 1 long distance code. The back spaces were ignored and the resulting number was 911-XXX-XXXX. Dialing 911 with a modem indicates you are a deaf person requiring help. The number was traced back to us (our rotary) and the first person to be called and asked about it was ME! (I made the first mistake, I made the second one. Sound reasonable... :-) It was found to be another machine doing the dialing, and was corrected.

In both cases the number written on the piece of paper was correct and the number entered in the computer was wrong. I wonder how often this happens. We are becomming more computer oriented (look at the number of modem ads you see, and the number of PC and PC clones that are sold.) Could this become a major RISK in the future, dialing wrong numbers for hours on end?

David Barto sdcsvax!sdcc6--\
barto@sdcsvax.ARPA ihnp4--!bigbang-!megatek!barto
seismo-!s3sun--/

Re: Mode C Transponders

<cbosgd!mhuxd!wolit@ucbvax.Berkeley.EDU>
Thu, 12 Mar 87 07:39:28 PST

Phil Karn writes:

> The simple fact is that your actions put others (like me) under involuntary
> risk, ...

What is "involuntary" about the risk? When you step aboard a plane, you know there's a risk that something will go wrong. No one forces you on.

Does your argument also apply to cars? Suppose I can afford to equip my Rolls Royce with one of those new radar-based automatic braking systems, making it much less likely that I'll plow into someone from behind. Now, don't I have the right to expect that everyone else out there will want to make *ME* safer as well, by installing these systems in their cars? The technology is there, we could certainly cut down the number of involuntary (think of all those innocent passengers) traffic deaths, if only people weren't so selfish and independent-minded. And we're not even talking here about systems that cost more than the cars themselves, unlike some of the aircraft collision-avoidance systems you want every plane owner to rush out and buy.

Anyway, this whole discussion has little to do with computer system risks, so let's shut it down. [AGREED. P.]

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

Automatic Landing Systems

Hugh LaMaster <lamaster@ames-pioneer.arpa>
Thu, 12 Mar 87 13:19:01 pst

There has been a lot of discussion on RISKS recently about air safety. I have three questions that perhaps someone out there has more detailed information about.

The first is the Automatic Landing System (ALS) that has been used in Europe. Could someone summarize what is known about ALS as far as RISKS is concerned? Is it (believed to be) a fail-safe system? Is it run by a digital computer (with software :-)) ? Are there steps being taken now to bring such a system to the U.S.?

The second question is about active controls on commercial jet transports. Somewhere, I read that the new McDonnell-Douglas MD-11 (follow on to the DC-10) will have relaxed aerodynamic stability, made possible by (naturally) active controls. What happens after a lightning strike wipes out all the avionics (it has happened)? It does not follow that if it is OK for the F-16, it is OK for a commercial transport. I assume that there won't be zero-zero ejection seats for each passenger.

The third question is whether there any completely fly-by-wire transports out there now? I have read that there is a version of the Airbus with fly-by-wire, but it didn't say whether it also had conventional controls. The same questions as above apply.

Hugh LaMaster, m/s 233-9, UUCP {seismo,topaz,lll-crg,ucbvax}!
NASA Ames Research Center ames!pioneer!lamaster
Moffett Field, CA 94035 ARPA lamaster@ames-pioneer.arpa

Phone: (415)694-6117 ARPA lamaster@pioneer.arc.nasa.gov

("Any opinions expressed herein are solely the responsibility of the
author and do not represent the opinions of NASA or the U.S. Government")

F-111 Losses

<fowler@rochester.arpa>
Thu, 12 Mar 87 12:47:03 EST

Back when I used do computerized cartography and terrain modelling I'd heard a story (unconfirmed rumor, interesting scuttlebutt) that some part of the F-111 lossage was due to active (and simple, low technology) countermeasures. In particular, one or more low altitude airbursts with an appropriate mortar round (chaff?) a couple hundred meters ahead of the plane would cause a very strong terrain-like radar return to suddenly appear. The G force limiting in the program was implicit, with the flight path obtained by filtering the observed terrain into a smooth curve. This worked great as long as the observed terrain is really static and doesn't do anything strange. When the terrain follower suddenly observed a "mountain range" appear immediately ahead of the aircraft it panicked by trying to climb over it. The resulting acceleration could be well outside specs.

Since the planes tended to reuse routes such as valleys, the implementation of this alleged countermeasure is simple. An observer with a phone alerts the mortar crews down route that a plane is coming and sould arrive in X seconds. The timing of the airbursts is non-critical. If the mortar crews get it right the wings fall off. If they are too far in front of the plane it pulls up hard anyway making it vulnerable to conventional AA. Even if the AA doesn't get the plane, the crew has just had a very disturbing experience. Their confidence in the terrain following system is shaken. Their mission plan might be screwed up possibly causing them to miss navigational checkpoints. They've got lots of excuses to abort and go home.

The immediate solution: program the system so that it ignores sudden changes in terrain. It wasn't obvious what would happen if there was a real hill on the other side of the burst. The smart money says don't rely on terrain following in hilly terrain.

-- Rob Fowler

Re: Computers in the Arts (Computer lighting)

Shannon Nelson <decvax!tektronix!reed!psu-cs!nelsons@ucbvax.Berkeley.EDU>
Wed, 11 Mar 87 15:52:41 PST

I've worked in several different theatres as a lighting 'techie', both as a stagehand and as the lighting designer. In at least two of the auditoriums I've worked in, the lights were controlled by a computer; one was computer

assisted, the other was fully computerized.

In the computer-assisted setup, the computer was used to control fast, highly complex fades and effects in addition to hand controlling of other fades qued on often 'inspirational' actors. This was a nice balance, as the operator could override the computer at anytime with a full set of manual controls (100+ channel 2 scene preset board).

In the fully computer controlled system, everything was done through the computer: setting levels, fade timing, special effects, etc. It had a ss/sd floppy drive on one side, and looked kinda like a tvi 910 terminal with several slider controls instead of keys. As long as the computer was operating correctly, it was useable. Unfortunately, it was originally installed wrong (by a regular (subcontracted) electrician, not a specialized theatre electrician) and was often unusable, aside from the "backup system". It was eventually fixed, but still, when it goes, it's gone.

There was a (half-baked) backup of all 96 channels tied to twelve controls (single scene, no presets). If the computer died from heat or power glitch, we'd turn the key over to 'backup' and hope that we could restart the computer and return to the correct sequence without too much confusion.

In such systems, the lights often cannot be done by hand because 1) there aren't enough hands (sometimes the case with over 100 seperate controls), and/or 2) the system wasn't designed to be overridden. In some cases, all that's left to human control are the follow-spots, which do little for flooding the whole stage.

Do I like working with computer lighting systems? Of course. They make my work as a designer much more exciting with the effects that are possible. Do I want full overrides, even if I don't have enough hands? You'd better believe it!! --

Shannon Nelson ...tektronix!psu-cs!nelsons

Search RISKS using swish-e

Report problems with the web pages to the maintainer

Search RISKS using swish-e

THE RISKS DIGEST

Forum on Risks to the Public in Computers and Related Systems

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

Volume 4: Issue 64

Monday, 16 March 1987

Contents

Computer-lighting board nearly causes WWIII

Mon, 16 Mar 87 16:07:51 est

With the recent discussion of computer-controlled lighting boards, I ask "How resistant to Electron Magnetic Interference should these boards be?" Not such as academic point as one would think. An audio engineer friend of mine related this incident:

He was running sound for the Broadway production of "A Chorus Line" a few years back. Then-president Ford came to a performance. Secret Service men everywhere. One by the sound board, one by lighting, etc. All is quiet until about the mid-point of the play. Then the Secret Service man standing by the lighting board (an early Nicholson model I believe) got a call on his walkie-talkie. To reply, he depressed the push-to-talk switch, sending out a couple of watts of RF, and Presto! the entire theatre was plunged into inky darkness. Chaos ensues, PERT guns are drawn, etc., etc. It completely wiped out the CMOS memory of the lighting board.

Questions: should mil-spec EMI resistance be built into only military equipment? Who would have thought that a lowly theater lighting board would be of critical national importance if for only a few moments? Could a high-tech John Wilkes Booth use some knowledge such as this for the next asassination attempt?

Brent Laminack (gatech!itm!brent)

Computerized telephone sales pitch meets emergency broadcast number

<itm!brent%gatech.UUX%ncar.csnet@RELAY.CS.NET>
Mon, 16 Mar 87 16:08:10 est

About 18 months ago here in Atlanta, a string of phone-related accidents caused much confusion and consternation in the lives of at least one family.

To begin with: one of these "computerized" telephone sales pitches was calling through a mid-town exchange offering "you have won a free Bahamas vacation. Just call xxx-xxxx!" As it was walking through the exchange, it hit an unlisted number. This phone was an emergency override number into the metro Atlanta cable television system. In the case of extreme emergency, the Mayor or head of the CD would call this number. The incoming phone line would override the audio portion of ALL cable channels currently in use. It was about 10:30 a.m., so there wasn't as big an audience as if it had been prime-time, but yes, all of Atlanta's cable subscribers were informed they had just won a free trip. Chaos ensued. Especially for the poor family whose telephone number was one digit different from the call-back number. Through no fault of their own they got one call every 20 seconds all that day.

Reducing the RISK of this repeating itself could take place at any step: Legislation limiting "computerized" sales pitches (this hasn't been done), a security code on the emergency phone number (this has been done) and for the poor lady getting the wrong numbers, not much. If any RISKS readers are unfamiliar with the design process that went into the design of the Touch-Tone (TM) keypad, it makes interesting reading. The designs were a speed vs. accuracy trade-off. The lady could only wish that The Labs had put a higher priority on accuracy.

This was sort of an information-age Orson Welles "War of the Worlds".

Brent Laminack (gatech!itm!brent)

Furniture risks

<Breisacher.OsbuSouth@Xerox.COM>
16 Mar 87 09:10:18 PST (Monday)

A friend of mine at a nearby company received an issue of their OA Bulletin which contained this little item:

Diskette Data Disappears in Desks

Data stored on diskettes may be lost if the diskettes are kept in the new Haworth modular furniture now in use in some offices. The drawer divider in the utility drawer of these units is held in place with a magnetic strip. These magnetic strips can erase the data stored on a diskette. Also, the task light ballast can erase the data stored on a diskette placed flat on the shelf immediately above the ballast.

To protect your data with these units, store your diskettes....

Reprise on the UK Government's ACARD Report

Brian Randell <brian%kelpie.newcastle.ac.uk@Cs.Ucl.AC.UK>
Mon, 16 Mar 87 15:52:01 gmt

A little while ago there was quite a debate in RISKS about the comments in the ACARD report concerning certification, and the use of formal methods, for safety-critical programs. Last week's Computer Guardian (an insert in the daily paper, The Guardian) carried a splendid article on this report by Keith Devlin, one of their regular contributors, who is in fact on the Faculty of the Department of Mathematics at Lancaster University. I and my colleagues here enjoyed its content and style so much that, even though it is somewhat lengthy, and the major points it makes are not new, we thought that it should be offered to RISKS, in its entirety, so that the rest of you can see what the UK national press is occasionally capable of!

DISCRETE CHARMS OF APPLICATION

Keith Devlin, The Guardian, 12 March 1987

Flicking through a report produced by a research advisory council to the Cabinet Office recently, my eye was caught by some rather amazing figures. The subject under consideration was the use of mathematical techniques to verify the accuracy of computer programs - surely a laudable aim if ever there was one. According to the committee who assembled this report, the current best practice in the creation of commercial software produces on average just one error in every one thousand lines of code in the final product. (How does one convey raised eyebrow using the written word?)

Given better verification techniques, the report went on, one could "realistically expect" an error rate of just one error per hundred thousand lines of code.

Well, in these days of PR hype one does become used to extravagant claims, but this one must take the biscuit. In a report that is presumably intended to shape future research directions, this is a ludicrous proposition to make. Worse still, the report did not stop there. The ultimate goal was, it appears, for the mathematician who certifies the said program as being "correct to within an error rate of 0.001%" to be henceforth held legally responsible for any future failures of the system (including the possibly lethal consequences thereof).

Now, while I am in complete agreement with the idea of professionals having a responsibility for what they do, the fact of the matter is that the committee who prepared this particular report have not the faintest idea of just what mathematics is about, and their faith in the notion of a "rigorous mathematical proof" would be touching if in the present context it were not so potentially dangerous.

To put it simply, a mathematical approach to the writing of computer programs is highly likely to result in better, more efficient, and more reliable programs, than would a less structured approach, but that is all. There can be no, repeat no, question of such an approach giving rise to a guaranteed product of the kind suggested. A mathematical proof of any reasonable length is just as likely to contain an error as is a computer program of the same length. Mathematics helps. It cannot cure.

The writers of the aforementioned report would do well to read the article on program verification written by De Millo, Lipton and Perlis in the recently published book "New Directions in the Philosophy of Mathematics," edited by Thomas Tymoczko and published by Birkhauser Verlag of Basel in Switzerland. Indeed, in spite of its possibly daunting title, I can recommend this book to anyone interested in mathematics and, in particular, its relationship to computing. Though - as with any compilation - there is some variation in the quality of the various articles, overall the book is worth getting hold of.

One particular chapter deserves special mention, and that is the account of the "Ideal Mathematician" written by Philip Davis and Reuben Hersh. As well as being hilariously funny, this succeeds in providing an uncannily accurate portrait of the typical, present day pure mathematician. (Indeed, I suspect that its humour is a direct consequence of its accuracy.) Read it if you want to discover what characters like me to for the greater part of our working day.

The Davis and Hersh piece is taken directly from their award-winning book "The Mathematical Experience," published by Harvester Press (Brighton) in 1981. If you have not yet come across it, make sure you do. It is, quite simply, the best general book on mathematics that has ever been written. So good, in fact, that when I heard that the same two authors had written a second book, I wrote at once to the publisher asking for a copy to review in this column.

When my copy of "Descartes Dream" by Davis and Hersh (Harvester, 1986) duly

arrived, what a disappointment! Gone is the life and vitality of the previous book. The short, unstructured chapters I found dull and unrewarding; the theme suggested by the title and the introductory chapters barely discernible in the rest of the book; and some of the writing is just plain bad. (I hope it is just the effect of trying to follow a huge success, and before long another gem will be on the way.)

Somewhat similar to "Descartes Dream" is another new book from Birkhauser: "Discrete Thoughts" by Mark Kac, Gian-Carlo Rota, and Jacob Schwartz. But where Davis and Hersh fail to convey any feeling of the vitality of mathematics in what they write, the assorted articles in this compilation are full of life, and consequently enjoyable to read. Anyone interested enough to read this column regularly should get a lot out of this book, written by three of the world's best mathematicians/computer scientists. So too should all those professional mathematicians who take their art too seriously, and those whose expectations of mathematics are far in excess of reality. But this is where I came in.

Last minute changes

Roy Smith <phrivax!allegra!phri!phrivax.phri!roy@ucbvax.Berkeley.EDU>
Sun, 15 Mar 87 08:40:57 EST

In RISKS-4.63 David Barto writes:
> I thus ignored the problem, went to USENIX, and while I was gone the
> problem was reported. (See what you get for making changes on a friday
> before going on a trip? :-)

Dave says this in jest, but it's got a lot more truth to it than he lets on. All the careful planning and testing you may normally do isn't worth a damn if you are willing to make last minute changes just before you lose control over the situation, whether that means making a change just before you go on vacation or adding the latest feature the day before you ship your product to the customer. It doesn't make much difference if we're talking computer software or toasters.

Roy Smith, System Administrator,
Public Health Research Institute, 455 First Avenue, New York, NY 10016

Risk in ``High'' Financing

Michael Wester <wester@aleph0.unm>
Thu, 12 Mar 87 22:17:09 MST

Excerpt from ``Risky moments in the money markets'' in U.S. News & World Report of March 2, 1987

According to the New York Fed, Wall Street's average daily volume of bank wire transactions totals at least $1.2 trillion---an amount equal to one quarter of the U.S.'s total annual economic activity---and could be as much as $500 billion a day higher, though no one really knows. Even at the lower figure, that's five times the daily flow since the start of the decade. Each

year, transaction volume leaps by nearly 25%, or double the annual growth rate in the 1970s. [...]

The obvious fear is a financial accident that could bring the system down. Banks must settle accounts daily, and a failure to pay up by one could cause a chain reaction of problems for others. Close calls in settling are more common than is generally known. A Federal Reserve Board official acknowledges the number of ``breathless moments'' averages 10 a year.

One of those scary scenarios developed in 1985, when the government-securities market was severely disrupted by a computer software ``bug'' at the bank of New York, preventing settlement for a day and a half. Only a $23.6 BILLION [my emphasis] emergency loan by the Fed got the wheels unstuck. [...]

Each day, billions of transactions move from country to country over a pair of wire systems: The Clearing House Interbank Payments System, called CHIPS, operated by 140 banks specializing in international finance, and the Federal Reserve Systems's Fedwire, which links 7000 domestic banks and does the bookkeeping for Treasury securities transfers among banks.

The electronic linkages make it possible for money to whiz from computer to computer so quickly that the same dollars can be used to finance up to seven deals a day, compared to two in times past when paper checks were the principal method of payment. [...]

One danger signal: Last year's daily transaction value was 24 times greater than the amount of reserves banks had on deposit with the Federal Reserve System, up from a 9.4 multiple in 1980.

It has become common practice for banks to go deeply into hock each day, often exceeding total assets in anticipation of payments they will receive before it is time to balance their books at closing. Such ``daylight overdrafts'' account for as much as $110 billion to $120 billion on the Fedwire and Chips. [...]

What makes the climbing debt even more unsettling is that payments move over CHIPS and Fedwire systems that [Gerald] Corrigan [, head of the New York Federal Reserve Bank,] describes as a ``hodgepodge of facilities, equipment, software and controls that have little in common with each other.'' Even if the hodgepodge is capable of handling the flow now, Corrigan and others worry about it remaining adequate if the transaction volumes continues to grow as astronomically as it has in recent years. ``The money spent on computer systems has not kept pace with the tremendous explosion in electronic payments,'' says a Fed official.

Michael Wester --- University of New Mexico (Albuquerque, NM)
~{anlams|convex|csu-cs|gatech|lanl|ogcvax|pur-ee|ucbvax}!unmvax!aleph0!wester

---

Risk at Crown Books

<srt@CS.UCLA.EDU>
Fri, 13 Mar 87 11:26:17 PST

Crown Books here in Los Angeles has taken to using an inventory control system where magnetic tags inside books are scrambled by passing them over a strong permanent magnet after the books are sold.

Then Crown Books started selling software.

Scott R. Turner UUCP: ...!{cepu,ihnp4,trwspp,ucbvax}!ucla-cs!srt
DRAGNET: ...!{channing,streisand,joe-friday}!srt@dragnet-relay.arpa

[We've had various hi-tech systems that were trivial to beat with lo-tech. This one converts remanence into remnants. PGN]

Human errors in computer systems -- another reference

Jack Goldberg <JGOLDBERG@CSL.SRI.COM>
Fri 13 Mar 87 12:49:19-PST

Jens Rasmussen "The Human As A Systems Component", chapter 3 in Human Interaction with Computers, edited by H.T. Smith and T.R.G. Green, Academic Press, 1980, paperback, London and New York editions. The book is a nice and diverse collection. Rasmussen discusses operator error, but not designer error. The chapter by Green, "Programming as a Cognitive Activity", touches on errors in program design. He criticizes a paper by Mills that implies that topdown design is the way to design good programs and praises a 1976 paper by Denning that rejects the proposition that the process of creating a well-structured design is (in general) well-structured.

Requests for War Stories in Scientific Programming

Dennis Stevenson <steve@hubcap.UUCP>
16 Mar 87 18:15:11 GMT

I have to give a pitch about software environments for developing scientific programs. One of the points that I would like to bring out is the "cost" of having a scientific model improperly coded and therefore spuriously rejected. Can anyone provide me with anecdotes (all names will be withheld) concerning this point? Also, if anyone has cogent arguments on the use of development environments/automatic programming in the scientific context, I'd appreciate them.

D. E. Stevenson csnet: dsteven@clemson UUCP: gatech!clemson!steve

---

TFR and F-111s

Eugene Miya <eugene@ames-nas.arpa>
Mon, 16 Mar 87 11:04:48 PST

In RISKs, you proposed some interesting scuttlebutt about mortar rounds and TFR. From what I know about the workings of radar, I would tend to be skeptical of the incident because radar systems have to take things like the

dielectric constant of materials in account [slightly more complex than this but I'm not here to talk about radar] ("earth" differs greatly from chaff, and moving earth (explosion debris) is even different than static; earth particle size is also significant), but what is interesting is what we don't really know about radar. I say, "I am skeptical," not "You are are wrong." What the radar/avionics person would tend to do would be to go empirically check this out. All aircraft are checked out in chambers to determine their base radar signature (empirically) because we don't have good models on radar return. So I would think the people at Hughes (Hugh Aircrash ;-) would have tested their radar under this circumstance as soon as it was proposed. BTW this is what is now also done for EMP testing.

--eugene miya

An Open University Text Book

Brian Randell <brian%kelpie.newcastle.ac.uk@Cs.Ucl.AC.UK>
Fri, 13 Mar 87 17:46:16 gmt

A colleague of mine recently lent me the following:

Understanding Systems Failures, by V. Bignell and J. Fortune
(Manchester University Press) 1984 (p/b). To quote from the blurb on the back:

> "This book outlines a common approach to the understanding of many different kinds of failure: failure of machines, of individuals, of groups and businesses.
>
> "A dozen case histories are discussed by the authors. They range from the accident at the Three Mile Island power station to the collapse of Rolls-Royce and the sinking of a North Sea rig, each a result of a variety of faults and failures. Failures are then analyzed through an approach based on the identification of the systems that failed and a comparison of these with a variety of standard systems.
>
> "The stories of many of these failures have never been written from such a perspective before, and this is the first time that a wide range of studies has been brought together to provide an understanding of failure in its widest possible sense.
>
> "Understanding Systems Failures is the set book for the Open University course T301, 'Complexity, Management and Change: Applying a Systems Approach'. It will be useful to students and teachers of management, business studies, administration and engineering."

The above seems a fair description to me. There is, as far as I can tell, nothing explicitly related to computers in the entire book, but it is nevertheless a book which might be of interest to the RISKS community - it would, for example, provide a good (and cheap!) source of quite detailed background factual material for students who were being required to analyze what part computers might play in decreasing (or increasing!) the likelihood and seriousness of various types of system failure.

Brian Randell - Computing Laboratory, University of Newcastle upon Tyne

UUCP : <UK>!ukc!cheviot!brian JANET : brian@uk.ac.newcastle.cheviot

US NEWS article on 'Smart' Weapons - questions and concerns

Jon Jacky <jon@june.cs.washington.edu>
Fri, 13 Mar 87 09:55:16 PST

The cover story of the March 16, 1987 issue of US NEWS AND WORLD REPORT is a long and colorfully-illustrated story on various high-technology tactical weapons. The story is somewhat informative but isn't real clear about which weapons already exist and are deployed, which are in development now, and which are just gleams in someone's eye. In particular, the article blurs the distinctions between what appear to be three rather distinct categories of weapons:

1. Precision guided weapons - The soldier selects the target and guides the weapon all the way to the target. These include the TOW optic fibre guided rockets and the various laser-guided bombs (which work because someone focuses light on the target, which the bomb homes in on). These are by now deployed all over the place and often work well, although they are not panaceas. A difficulty is that the soldier must often remain exposed during the whole flight time of the weapon.

2. "Fire and forget" weapons - The soldier selects the target, but the weapon guides itself to the target. This is significantly harder. The most effective examples seem to depend on the target making itself very conspicuous, for example the HARM anti-radiation missiles that home in on radar beacons. The article also describes AMRAAM, an air-to-air missile of which it is said "a pilot can fire as soon as he detects an enemy aircraft. He can immediately steer clear while the missile tracks and kills the enemy with no further help." The story says AMRAAM is "costly and controversial" but is "now being tested." Is this for real? I vaguely recall hearing about AMRAAM off and on for many years, and thought it was in a lot of trouble, a bit like the Sgt. York.

3. Autonomous weapons - The weapon itself selects the target. I have a lot of trouble with this one. For one thing, it is obviously a lot more difficult technically than even "fire and forget;" The article rather blurs this distinction. The article says,

"Smart bombs that require human control might not be good enough. ... A simple stick-figure picture of a target, such as a railroad bridge, is put into one "autonomous guided bomb" under development. Launched at very low level with a strap-on rocket, the bomb flies a preplanned route until it sees something to attack that matches its computer's picture."

Does anyone recognize the project refered to here? Is this thought feasible? Based on my understanding of the state of the art in image understanding, I would have thought not. Does this possibly represent some reporter's

understanding of some rather speculative document like the 1983 DARPA Strategic Computing Report?

Another autonomous weapon which is evidently farther along is SADARM:

"The Army's Sense and Destroy Armor (SADARM) smart-weapon system uses advanced radar, heat sensors, and a miniature onboard computer ... Fired from artillery, ... the submunitions, each a small, self-contained weapon, would pop a small parachute and spin slowly down as it scans for telltale signatures of self-propelled guns. Once it sensed the presence of a target, it would aim for the center and fire an explosively formed slug of metal that slams into the lightly armored top of the vehicle, filling the crew compartment with a hail of deadly shrapnel."

What are these "telltale signatures?" Are they all that discriminatory? Elsewhere, the article implies that distinguishing tanks from trucks and jeeps is not much of a problem. Is that true, _in the context of this kind of weapon_?

The article strives for journalistic balance in the usual way: Proponent A says these are necessary and would be effective, critic B charges they may be ineffective and we should not become too dependent. What I find missing is the notion that perhaps such judgments need not be based on personal opinion, that it ought to be possible to design tests that determine these things. That is, maybe A is right and B is wrong (or vice versa). I assume the people who work on these understand that, but the concept never really appears in the article. Also, the article implies that the strategy and doctrine of relying rather heavily on this kind of stuff is almost dogma by now, rather than still being provisional and much debated in strategy circles. Is that true?

The article is especially good in in explaining why such weapons are thought necessary:

Population trends tell the story ... West Germany has the world's lowest birth rate. ... By 1994 the draftee pool will shrink nearly in half. In America, political realities impose an equally inflexible obstacle. "How far do you think a President would get who wanted to reinstate the draft, expand the standing armies by three or four times, and deploy a major portion of that force overseas?" asked Joseph Braddock (of the defense think-tank, BDM). "We don't have much choice," adds former Defense Secretary Harold Brown. "We've got to choose quality over quantity."

-Jonathan Jacky, University of Washington

Search RISKS using swish-e

THE RISKS DIGEST

Forum on Risks to the Public in Computers and Related Systems

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

Volume 4: Issue 65

Thursday, 19 March 1987

Contents

---

risks@csl.sri.com, sdcrdcf!decvax!ucbvax!CSL.SRI.COM!risks
Subject: Largest computer crime loss in history?
Date: Tue, 17 Mar 87 07:50:01 -0800
From: kremen@aerospace.aero.org

According to page 22 of March 16th's Wall Street Journal, Volkswagen may have lost over 259 million dollars due to foreign-exchange contract fraud. According to the article, the fraud involved "the erasure of computer data and tampering with computer programs."

health hazards of poorly placed CRT screens

Gregory Sandell <sandell@tcgould.tn.cornell.edu>
Thu, 19 Mar 87 10:55:09 EST

I want to share an experience that I am having with a health problem connected with my work. I am a programmer and spend a lot of time at a CRT. I am not technology-phobic, but I have been enlightened by my chiropractor that CRTs can be dangerous. Many CRTs in my work situations are placed low enough so that my neck must be tilted at a *very slight* angle. I have been experiencing neck stiffness on and off over the last two years...it frequently bothers me for as much as a week at a time. My chiropractor tells me that holding my head in a fixed position at that angle --- even as slight an angle as it is --- for a long time is probably causing that stiffness. It so happens that I must hold my head at nearly the same angle when I play piano and look at music on the music rack of the piano. I am changing my behavior quite a bit; I have raised the CRT on my main workstation so that it is at eye-level; if the computer I am working at can't be adjusted that way, I look down with my eyes instead of using my neck. For piano playing, I tape the music up higher on the rack, or just memorize things in order to avoid holding my head in that deadly fixed position. I think that it is helping.

If this doesn't afflict you, then that's great. But I would guess that in general the position of CRTs in most work areas are placed with complete disregard for healthy neck position, and as a result many programmers are in danger of getting this reaction. Maybe 10 years from now we'll see photographs of computer work environments and experience the same kind of dismay we get when we see photographs of turn-of-the-century sweatshops. Think of it this way: would you want to watch *television* with your neck at that angle (not to mention with the screen so close to your face)?

[RISKS has explored this topic several times. The evidence is mounting that there are hazards in using terminals. Among my acquaintances, I have recently run across an orthomolecular physician who after setting up a new color display and working on it for 16 hours straight discovered serious physical damage to one of his eyes. Another person (with serious candida albicans problems, and thus greatly increased sensitivity to his environment) finds a strong sensitivity to fumes from his PC -- possibly from the power supply. Headaches, backaches, neckaches, and certain internal problems are also linked or aggravated by extensive terminal use. So, perhaps in the future terminals will come with a warning: computers may be habit forming and hazardous to your health. PGN]

Re: Computerized telephone sales pitch meets emergency

<Frankston@MIT-MULTICS.ARPA>
Tue, 17 Mar 87 06:46 EST

broadcast number

To: itm!brent%gatech.UUX%ncar.csnet@RELAY.CS.NET
cc: risks@CSL.SRI.COM

While I find computerized sales pitches obnoxious, I find it amazing that the Atlanta cable TV system would have a dial-in number that overrides the system without a password required. It is very easy to misdial a phone number. But, as has been a theme of my earlier letters, the phone system represents a misunderstood technology. A secret phone number itself does protect against certain classes of malicious attack, but is very vulnerable to accidents. Given the number of wrong numbers I get on my phone, I'm surprised that Atlanta has not already been treated to confused callers broadcasting to the city.

[There are indeed many risks associated with unlisted phone services. A variety of existing services offered are accessible either accidentally or intentionally from unexpected sources. (Steve Jobs' latest endeavor also has a whole bunch of associated risks.) The phone service that lets you call your home computer and then punch some more digits that turn on the oven or unlock a door for the delivery man is one example. The phone service of having your pacemaker battery checked remotely by a computer that interrogates it in a diagnostic mode is another. Believing that an unlisted phone number will not get called is of course utter folly. My unlisted home computer number gets about a call-a-day's worth of wrong numbers. The scanning phone solicitors are extremely agressive. In the Atlanta case we again have an example of a risk that was not anticipated, and discovered only after it was accidentally triggered. PGN]

---

phone key-pad speed vs accuracy

Andrew Klossner <andrew%hammer.tek.com@RELAY.CS.NET>
Wed, 18 Mar 87 12:46:52 PST

My new unlisted phone number contains two adjacent '9's. Just about all of the wrong numbers that I get are caused by somebody's '9' key double-clicking. I'm giving serious consideration to changing to a phone number with no repeated digit.

[I hesitated before including this one, but then decided there is an interesting problem in coding theory. Perhaps phone companies could offer an eight-digit number for those seeking a redundant digit to reduce wrong numbers. But, the algorithm would have to be carefully chosen to detect as many transpositions, accidentally repeated digits, and adjacent (with respect to the keypad and the rotary dial) digits as possible. I would subscribe at a reasonable price. PGN]

ATM experience

Joseph I. Herman (Joe) <DZOEY@UMD2.UMD.EDU>
Thu, 19 Mar 87 19:13:06 EST

A friend of mine deposited her paycheck using the bank's ATM machine. When

she signed her paycheck, she also wrote the account number on the back. Unfortunately, she interchanged two numbers, so the check was deposited in some random person's account. The ATM machine gives her a receipt that basically says that her deposit was accepted, so she went off and assumed that the check was deposited correctly. Well, of course the bank didn't bother to verify that the account number written on the back of the check matched either the account number printed on the ATM slip (included with deposits) or the account name. They just blindly took her word for it.

After quite a hassle and a couple of bounced checks, things were straightened out, but it took quite a bit of time and much embarrassment.

I can think of two problems here. The redundancy of having a name associated with your account and the further redundancy of having the ATM print a special deposit slip to be included with each deposit is pretty useless if people aren't going to check them. The other problem is it introduces an incentive to *not* put your account number on the back of your check, and instead depend on the ATM slip to furnish this information, thus increasing the dependance on automation.

By the way, the bank stated that it was not at fault here. I'm not so sure, after all, it should have detected the discrepancy.

Joe Herman

Computerized Telemarketing

Rob Aitken <aitken%noah.arc.cdn%ubc.csnet@RELAY.CS.NET>
18 Mar 87 1:50 -0800

Regarding the recent discussion of the RISKS of computers and telephones: Several years ago, when I lived in Victoria B.C., the local telephone sales organizations (e.g. "Buy the XXX vacuum cleaner") purchased a computer which called up various numbers to make its pitch. The problem with the system was that it would not release the line, even if the potential customer hung up. In one case, a mother was prevented from calling for an ambulance while her child was choking. Fortunately, the child survived. Soon after, laws were passed requiring the dial-up computers to hang up when the customer did.

Rob Aitken, Alberta Research Council, Calgary AB

[We've had several very similar cases in the past.
This one is included for the record. PGN]

Submission impossible?

<NEUMANN@CSL.SRI.COM>
Tue 17 Mar 87 10:42:32-PST

In the cyclic process of deciding on how much to include in RISKS, I have once again been turning up the threshold due to an increase in somewhat marginal material. I realize that the masthead guidelines are in EVERY

issue, and therefore perhaps only new readers pay attention to them. On the other hand, I believe that the RISKS Forum serves a very useful purpose in tolerating open discussion, even when some of it is not quite accurate -- we all learn from the ensuing discussion. Therefore I hate to stifle openness. But I also get complaints when RISKS issues get very long or very frequent -- and besides it is tough on me trying to keep up with all of you when you get into FLOOD MODE on a popular issue. So, try to stick to the guidelines.

By the way, I received messages from ONLY TWO of you questioning my command of the English (american) language in the masthead item in RISKS-4.63:

++++ NOTE: We are starting to mine out old loads rather heavily ++++
++++ of late. PLEASE try to be MORE CONCISE and LESS REPETITIOUS! ++++

The use of "load" instead of "lode" was quite intentional (I try not to explain or even highlight all of my puns), and might even be interpreted by some of you as an editorial comment.

Risk at Crown Books

Christopher Garrigues <7thSon@STONY-BROOK.SCRC.Symbolics.COM>
Wed, 18 Mar 87 09:51 EST

When I was in Junior High School (about a decade ago), I was working in the school library when they instituted the magnetic tag approach to security. Well, naturally, those of us who worked in the library, immediately started trying to determine how to defeat the system. It didn't take us long to discover that a hard rap on the spine of a book against a desk or table sufficiently scrambled the magnetic elements that the book would pass through the detector. Because the system is so easy to defeat, it's actually easier to steal books now because you can be reasonably sure that the bookstore employees have enough trust in their system not to watch what people carry in and out.

> [Computer/technology related? Well, it is a fine example of the dangers of trusting a technological solution... PGN]

Altitude Encoders... expensive for some

<LIN@XX.LCS.MIT.EDU>
Wed, 18 Mar 1987 20:09 EST

> From Ronald J Wanttaja:
> Ann Landers has a right to her opinion. But what do I say when someone mentions that "Ann Landers says we gotta ban the little aircraft?"

You explain to them why banning little aircraft is not the solution. I agree that it is difficult, but telling them to go away (as I am sometimes inclined to do myself) is a sure way to polarize the community.

> Similarly technical decisions are best left to those technically qualified.

Perhaps. But when the "unqualified" (such as Congressmen [...]) are ultimately the ones who make the decisions, you ignore them at your own peril.

RTD Ghost Story: a Phantom Warehouse

<Nickell.pasa@Xerox.COM>
Wed, 18 Mar 87 08:21:21 PST

LOS ANGELES TIMES, March 18, 1987
RICH CONNELL and TRACY WOOD, TIMES STAFF WRITERS

The financially troubled Southern California Rapid Transit District has created a phantom warehouse to "store" more than $1 million in lost, stolen or misplaced bus parts, RTD employees have told The Times.

The dummy warehouse, as some RTD employees also all it, was devised nearly a year ago and exists only in the RTD's computers -- a kind of accounting limbo for lost materials that at other transit agencies are promptly acknowledged and written off as losses. RTD workers charted that the ghost warehouse, labeled "SD14", is symptomatic of management efforts to hide mistakes with little regard for public cost.

"It makes [RTD middle managers] look good to higher-ups ... . You're not losing as much money on paper," said one warehouse employee familiar with the system.

John Richeson, RTD's assistant general manager, the district's overseer of inventory, said he learned of the non-existent warehouse only last week as a result of inquiries by The Times. However, he defended the bookkeeping maneuver as a good idea for handling "inventory that is not in the location it is supposed to be."

RTD managers acknowledged that the non-existent warehouse is an unusual bookkeeping procedure, but they insisted that it is neither improper nor deceptive. Richeson said that to characterize the district as hiding its inability to control inventory is "not the proper interpretation."

The list of missing parts in the phantom warehouse has grown from zero nearly a year ago to more that 500,000 items worth $1.28 million in bus and office supplies on hand. RTD officials said that hunting down the missing supplies and trying to determine how much has been stolen and how much has been misplaced has been a low priority because the search would be too expensive and time consuming.

"The dollar value certainly is not substantial in terms of the overall inventory or the overall volume of things we are doing," Richeson said.

However, the fuzzy status of materials moved to the non-existent stock area creates other problems. It is now more difficult for transit police investigators to know quickly when parts are truly missing and possibly stolen, said RTD Police Chief James Burgess.

"That's one of the problems we do encounter with this system," he said. [...]

RTD managers inserted the phantom warehouse into the district records after a systemwide inventory of bus parts was taken last April. The inventory supposedly produced a complete tally of RTD bus and office

supplies, from which accurate computer records of parts on hand were produced for the first time.

However, several sources familiar with warehouse operations said the inventory served mainly to reveal the lax controls on parts and supplies.

"It was a complete disaster," said one, explaining that a lot of material listed in inventories could not be found.

In other instances, RTD officials acknowledged, inventories that were on hand may have been overvalued.

"The inventory was meaningless," said another source who participated in the inventory [...]

Almost immediately after the inventory adjustments were made to the books, parts began disappearing again, causing new problems.

A computer system that is supposed to automatically replenish parts when they are needed began refusing to place some orders. Since disappearing parts were not being removed from inventory lists, the computer showed the district had those parts on hand. But stock clerks checking the shelves were unable to find them.

Faced with a parts-purchasing bottleneck that could sideline badly needed buses, district employees began making expensive rush orders for special overnight deliveries from manufacturers.

Partly in response to this new set of inventory problems, RTD management placed the phantom warehouse on its books. They listed it as SD14, the kind of computer label used to designate an actual warehouse at a specific location. SD14 was inserted in a column of real warehouse listings, with nothing other than its number to set it apart, for example, from SD10, the computer designation for a storeroom at a bus yard near downtown Los Angeles.

ELECTRONICALLY 'SHIPPED'

Wayward parts were thereafter electronically "shipped" to the new warehouse, freeing the central computer system to reorder parts to keep the system's 2,800 buses running.

In addition, the fake storage area has eased the pressure on managers to account for missing parts. In the past year, they no longer have had to "write off" all the parts they could not find and were able to minimize unexplained losses in their budgets.

RTD officials insist that the chief purpose of the phantom warehouse was to ensure that a detailed investigation of missing materials could be made. Maynard Walters, RTD director of purchasing who authorized creation of the ghost storage depot, recalled telling his staff, "I don't want it [written off as a loss]. I want it put in an account and held there so I can have a report on why it's not there."

However, after 11 months, officials say they have not had the manpower to track down all the errant parts and supplies assigned to SD14.

"We have a certain amount of personnel that we can spend finding all of these things...," said James Connolly, the RTD's materials manager, who set up the fictitious warehouse.

Gradually, SD14 grew until it had three or four times the parts and inventory value of other satellite stockrooms.

ARGUMENTS ERUPTED

So real did SD14 appear, that for months, warehouse clerks and

mechanics unsuccessfully tried to retrieve needed parts from it -- and even got into arguments with higher-ups over why supplies stored there could not be delivered.

"I couldn't figure out what it was," one RTD warehouse worker said. "I'd look on the computer screen [for parts]. It would say nobody has them but SD14. I'd say why can't we get them from SD14. [Eventually, I was told] SD14 doesn't exist."

As time went on, the phantom storehouse became a running joke among warehouse workers. The instant any part was misplaced, someone would suggest, "look in SD14," employees said [...]

NEW FACILITY

As part of a sophisticated parts-tracking system at the new facility, computer-guided robots will store and retrieve all parts, keeping an accurate, running inventory as they go, RTD officials contend.

"It's just like night and day in terms of the ability to control things," Richeson said.

Other RTD employees are less confident. They point to management shake-ups and earlier highly touted state-of-the-art systems that have not solved inventory control problems.

One RTD worker, referring to the new high-tech warehouse, said, "There'll be problems there we haven't even anticipated, that will be magnified tenfold."

Search RISKS using swish-e

THE RISKS DIGEST

Forum on Risks to the Public in Computers and Related Systems

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

Volume 4: Issue 66

Sunday, 22 March 1987

Contents

Question for Risks Readers on Information Overload and Technology

Dave Taylor <taylor%hpldat@hplabs.HP.COM>
Thu, 19 Mar 87 23:50:10 PST

I'm working on a paper entitled:

> Overcoming Information Overload with Technology
> (Why It Can't Work) ,

talking about mostly (from the abstract):

> Most of the solutions that are commonly posed to the problem of
> information overload are to ``build better mousetraps'', the

> hope being that the technology will catch up and allow us to
> sift through enormous amounts of data easily. I believe that
> not only is this thinking flawed, but dangerous, and discuss the
> inherent problems from both a technological and cultural perspective.

and would be most interested in any thoughts readers of this digest had about this subject matter. (It's for the upcoming Directions and Implications of Advanced Computer Systems conference in Seattle) (not that I've had it accepted yet, or anything...)

I'm especially interested in horror stories people could tell me about relying on information filtering systems and finding that they actually weeded out critical information... Thanks!

-- Dave Taylor <taylor@hplabs.HP.COM>

Fumes from PC's

Lauren Weinstein <vortex!lauren@rand-unix.ARPA>
Fri, 20-Mar-87 08:52:42 PST

The most likely cause of a problem is OZONE. Created by "high" voltages, it is commonly associated with sparks and (particularly A.C.) motors. Given that the average PC circuit board or disk doesn't do much sparking (one hopes!) a possible culprit is the fans commonly on power supplies or other equipment in PC's. These are usually driven by A.C. motors. If the fan(s) brushes are sparking internally (this will generally be invisible from outside inspection), considerable ozone can be created--this is very irritating to some people and generally not great for anyone (ozone is one of the commonly measured components of air pollution).

--Lauren--

Re: health hazards of poorly placed CRT screens

Brinton Cooper <abc@BRL.ARPA>
Fri, 20 Mar 87 13:00:33 EST

One of the most common causes of neck pain is anxiety (stress). Excessive worrying about daily use of a CRT might bring on or exacerbate neck pain, might it not?

_Brint

How to lose your ATM card

Jan Kok <KOK@YUKON.SCRC.Symbolics.COM>
Fri, 20 Mar 87 11:22 EST

Recently an ATM machine (operated by the CA$H Network) confiscated my card. Here's what happened:

I entered my password, but didn't press the keyboard hard enough, thus losing the first digit. Realizing what had happened, I pressed CANCEL, and the machine ejected the card. Since I just wanted to try again, I poked the card part-way back in, rather than taking the card out as the machine instructed. The machine didn't "accept" the card, i.e. the motor which normally pulls in the card didn't operate. At that point I realized the machine wanted me to take out the card, but by then there wasn't enough of the card exposed for me to get a grip on it. After I had fiddled with it for about a minute, a helpful bystander pushed the card all the way in, and the machine promptly informed me that it had taken the card and that I should contact my bank. I guess the machine thought I was tampering.

By the way, the person at the bank told me that when an ATM machine seizes a card, it chops it in two, so I have to wait a couple of weeks for a new card. Meanwhile I've opened an account at another bank so I'll have another card for a different ATM network.

Re: ATM experience

<Bruce_McKenney%itsmts@CSV.RPI.EDU>
Fri, 20 Mar 87 10:56:54 EST

In reference to the person whose ATM deposit went into the account written on the back of the check, rather than that associated with the ATM card:

A few months ago, I had precisely the opposite experience: after carefully filling out the deposit envelope, checking the "Checking Deposit" box and writing the account number for the checking account, I inadvertently punched the "savings deposit" button on the machine, and sure enough that's where it went, much to the detriment of checks drawn over the next week. Though I confess I failed to study the deposit receipt closely enough to detect the discrepancy, I was a bit surprised that the conflicting information didn't set off red flags somewhere.

A query directed at one of the people who opens those envelopes received the response "Oh, we never look at what's written on the envelope". I never did receive a satisfactory answer as to:

1) why, given a choice, information requiring 10 penstrokes (and presumably a bit more thought) should be ignored in favor of information requiring only a single button-push (presumably much more susceptible to accident)
2) (the larger question) why redundant information which could be useful for cross-checking is requested but ignored. It seems to me that this latter is a classical issue in hardware, software, and humanware systems.

Re: Increased Telephone Switching Capabilities

tty08

Fri, 20 Mar 87 11:13:37 pst

A recent article ("Telephones: Learning Some Manners"; The Economist, March 14, 1987, pg. 82) discusses a pilot project at three exAT&T local operating companies of a system called Local Area Signalling Service (LASS). The new technology is a "line history memory" at the originating line's switch which records the number dialed. This number can be queried by the receiving line's switch. Some of the capabilities require a new instrument with display but most do not. The article quotes $5/month marginal cost.

The big gain is in reducing the current invasion of privacy. Most people wouldn't admit physical persons into their home before determining their identity, but we don't know who we are going to talk to until we answer the phone. Other tricks include:

Got a busy signal? Punch a code for automatic reconnect. When both caller and called lines are free, the system calls the caller and asks if the call should be completed. Several calls may be pending.

Pick up the phone just in time to hear the other end disconnect? Ask your local switch to call him/her back.

The incoming identifier phones would be useful to mail order houses etc. to verify the origination of a call, as well as the privacy application. (The article also points out that it will prevent calling your spouse from a bar with a fib about working late.)

The local switch could also contain a "screen list" of numbers for special treatment; selective call forwarding, call waiting, or exclusion. (The original system gave a message "At the customers request, your call is not being completed" to excluded callers. This annoyed a lot of people, so it was changed to a "fake" ring-no-answer.)

The article also points out that over half of all nuisance calls are placed from home. The new system will discourage that sort of thing.

I discussed this article with a friend, who made two interesting assertions:

1) The information (calling #) is already available, and is encoded somehow just prior to the ring spike on the receiving line.

2) He was told by manufacturers of telephone sets that a feature to display this information on the recipient telephone was against current FCC regulation.

Such a system opens and closes many abuses of the phone system. The article mentions nuisance calls and mail order verification. I don't see any obvious risks to the new features, but I can imagine weird combinations of screens leading to unintended results.

Can anyone comment on my friend's assertions, or know which three operating companies were involved in this project?

Dan Graifer

Releasing the phone line

<lll-crg!micropro!edg@seismo.CSS.GOV>
20 Mar 87 11:20:58 PST (Fri)

The issue of automatic callers releasing the phone line is actually a people issue rather than a technology issue. Most telephone companies will release an incoming call when the recipient has hung up for about 15 seconds. This does not depend on the caller hanging up. When I was a kid, we knew that we could move from one phone to another as long as we did so in less than 15 seconds (and were the recipients of the call) rather than the callers.

The problem comes when the call is unwanted. The recipient generally hangs up for as long as it normally takes to get a dial tone (1-2 seconds) and then goes off-hook, to "check" and make sure that the call was dropped. Naturally, it was not. The recipient goes on hook for another two or three seconds and checks again. Call still connected. Panic sets in and a feedback loop ensues. The recipient is unable to drop the call, not because the line is being held from outside, but because s/he does not know how to do so.

When I get an unwanted call, I hang up, and walk away. I admit that the parent trying to call an ambulance does not have this presence of mind, but in truth, it would work.

This is not to imply that I approve of automatic telephone solicitors. I consider them to be one of the few things worse than human solicitors.

-edg

Automatic dialing devices in Canada

Michael Wagner <wagner@gpu.utcs.utoronto>
Sun, 22 Mar 87 12:58:12 EST

I was recently cleaning up my files in preparation to moving to Europe for a year, and came across the following insert in a phone bill from some time ago (a year or two, judging by the stratigraphy). I thought it might be of interest to RISKS readers. My phone supplier is Bell Canada (I'm in Ontario).

> Are you offended by recorded telephone solicitation calls?
>
> To help regulate the number of unwanted phone calls coming into your home or business, ground rules have been established by the Canadian Radio-television and Telecommunications Commission (CRTC) governing automatic dialing and announcing devices (ADADS) _when used for telephone solicitation purposes_. [italics in the original..mw]
>
> ADADS are ... [explanation of what they are and what they do...mw]
>
> Now, before the pre-recorded message starts, you must be informed

of the nature of the call, the identity of the caller, and that you may end the call by hanging up.

Within 10 seconds of [your] hanging up, the ADAD must disconnect from the line. ADAD calls may be made only between 9:30-20:00 weekdays, 10:30-17:00 Saturday, 12:00-17:00 Sunday.

[two more paragraphs explain how and to whom you complain about violations, and the fact that organizations using ADADs have been warned what violations will do to their phone privileges...mw]

Overconfidence in Airplane Computers?

<TMPLee@DOCKMASTER.ARPA>
Sat, 21 Mar 87 14:29 EST

Somehow, having just had the time to catch up on the last dozen issues or so of Risks, the following seems appropriate. My last flight back from DC Thursday afternoon had one of those chatty pilots, which I'm never sure I appreciate or don't. Anyway, once we were well underway he boasted about all the wonderful features of the 757. (I'm not knocking the plane: as a passenger I like it.) After talking about how the thrust is half the weight (mass, technically) of the loaded plane, the seven-color radar that spots precipitation and turbulence, etc., he then added (paraphrased), "and this plane has over a 100 on-board computers for your comfort and safety; for all you know you may be sitting on one right now." That almost ruined the whole flight! (at least, I pondered over it quite a while.)

Ted

[Seat-of-the-pants computing? PGN]

Search RISKS using swish-e

THE RISKS DIGEST

Forum on Risks to the Public in Computers and Related Systems

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

Volume 4: Issue 67

Tuesday, 24 March 1987

Contents

Winch is the greatest risk in a theater?

Dave Wortman <dw@csri.toronto.edu>
Mon, 23 Mar 87 15:15:11 EST

Look up if you want to see the real RISKs in many theaters. The failures in computer lighting systems discussed recently may cause inconvenience or economic loss, but failures in the computerized winch systems used to "fly"

scenery have the potential to cause serious bodily harm.

The typical arrangement for flying a piece of scenery is to attach several lines (e.g. 3/16 wire rope) to it, run these lines up to the stage ceiling around pulleys to the drum of an electrically powered winch. The winch is controlled remotely either manually or in more sophisticated systems by small computers. These computers can be preprogrammed with the flying sequence for an entire performance in a way very similar to the programming of lighting systems. The scenery being flown can be quite heavy. The electrical winches are supposed to be failsafe, i.e. a brake is automatically applied if power or control is lost.

One of the first such systems was installed in the Loeb Theater at Harvard in the early 1960s. It had several interesting failure modes including one in which the winch went into "full speed up" mode and tried to pull the scenery through the pulleys in the ceiling. This continued until the wire rope snapped and the scenery went into free fall.

Dave Wortman, Computer Systems Research Institute, University of Toronto
ex-stagehand and -theatrical-rigger

> [I presume there were no cases of rigger mortis. But,
> perhaps there were winch-healed wipers on the motors. PGN]

DC9 Computer Failure

<Boebert@HI-MULTICS.ARPA>
Mon, 23 Mar 87 11:16 CST

Somebody mentioned a NY Times article about our good 'ol Northworst Airlines that described an incident in which there was an all-channel failure of the computer system on a DC9 (must have been an MDA80) which led to the loss of all attitude display. Supposedly the airliner was led into Toledo airport by a general aviation aircraft (!). Anybody have any details on this?

Health hazards associated with VDU use: eyestrain

<munnari!basser.oz!john@seismo.CSS.GOV>
Sun, 22 Mar 87 14:18:57 EST

Gregory Sandell's submission prompted me to mention the main problem I have had with VDU use; namely, eyestrain. I used to find that after a day at work my eyes would be very tired. About a year and a half ago, I saw an article on the net suggesting that a good way to reduce eyestrain associated with terminal use was to reduce the amount of light striking the screen as much as possible. So, my office-mate and I implemented the following measures (adapted from suggestions in the original article, which unhappily I no longer seem to have):

* Keep all windows well covered during daylight hours.

We have venetian blinds on our window and closing them completely is reasonably satisfactory. It would be better if we could exclude even more light, though.

* Turn off all overhead lighting.

Our room is lit by fluorescent lights which are quite bright. With them turned off and the blinds closed, it gets reasonably dark. The darker the better.

* Use desk lamps, but _keep light from them OFF the screen!_

We each purchased two spring-arm type desk lamps to illuminate the work area on our desks. Reading material on the desk is probably easier than before, as the desktop is actually better illuminated now than it was by the overhead lighting.

Our experience with this has been very positive indeed. Both of us have completely ceased to suffer from eyestrain. And I also find the dimly-lit environment to be much more relaxing than it was when it was brightly illuminated.

I would like to thank the poster of the original article, whose name I unfortunately don't know, and thoroughly recommend this approach to anyone who suffers from eyestrain due to VDU use.

John Mackin, Basser Department of Computer Science,
University of Sydney, Sydney, Australia

john@basser.oz.AU (john%basser.oz@SEISMO.CSS.GOV)
{seismo,hplabs,mcvax,ukc,nttlab}!munnari!basser.oz!john

[As a related comment, I have some friends who are very sensitive to fluorescent lighting, which can give them monumental headaches. (Several of them have conducted reasonably careful experiments that seem to pinpoint that sensitivity.) I will not speculate in this forum on what the possible neurophysiological causes might be, although the incomplete light spectrum is a likely candidate. PGN]

Who called? (Re: RISKS DIGEST 4.66)

Jerome M Lang <jmlang%water.waterloo.edu@RELAY.CS.NET>
Tue, 24 Mar 87 12:19:53 est

In the last digest mention was made about the possibility of learning the phone number of the caller. This raises the question of what is done when the caller has an unlisted phone number (usually for very good reasons).

Jerome M. Lang || jmlang@water.bitnet jmlang@water.uucp
Dept of Applied Math || jmlang%water@waterloo.csnet

U of Waterloo || jmlang%water%waterloo.csnet@csnet-relay.arpa

[Clearly one would have to suppress that information -- under certain circumstances -- although it is clearly needed for the 911 computers. This gets into the problem of secure databases and how difficult it can be to prevent inferences from being drawn if you are going to hide information selectively. Lots of nice research has been done, but basically this is a very difficult problem once you take the blinders off. PGN]

Car Phone Intercept -- implications of captured data

Alex Dickinson <munnari!augean.oz!alex@seismo.CSS.GOV>
Tue, 24 Mar 87 09:02:16 CST

On Sunday 22nd March an Australian activist group using a radio frequency scanner intercepted and recorded an unencrypted car phone conversation between a federal opposition shadow minister and a state opposition leader (both members of the Australian Liberal Party). The conversation referred to the Liberal Party federal leader in what has been euphemistically termed `colourful language' and discussed his intended political demise. The group released the tape to a Melbourne newspaper that proceeded to publish a number of juicy excerpts.

Today the federal shadow minister was fired from his party post, and the chance of an election being called by the Prime Minister to take advantage of opposition confusion was regarded as having doubled from 15 to 30%.

Federal police are considering whether to press charges under the Telecommunications Act that broadly covers such interceptions. The fine? $5000 maximum. Good value for altering the course of the country's politics, although it's not clear that that was the intent.

Alex Dickinson

Re: Increased Telephone Switching Capabilities

Michael Wagner <wagner@gpu.utcs.utoronto>
Tue, 24 Mar 87 16:41:19 EST

I can offer two pieces of information, neither of which answer the questions completely.

1) the 911 emergency number in Toronto displays the number from which a call was made. It does this for a wide variety of originating exchanges (but I don't know if it does it for all exchanges). I have been told, by people who are more knowledgable about phones than I, that the number is sent on the same circuit as the phone call. They claim that almost no gymnastics were required to make this work.

(The phone company also makes a database of phone numbers and addresses available to the emergency service, so that numbers are quickly turned into street addresses. That clearly wouldn't be available to the average

business or home. But that is a different matter.)

The implications are that (a) exchanges send the origination phone number along with the call, and (b) exchanges can relatively trivially send the information to the customer phone, and (c) the customer phone can decode the information while the phone is still ringing, and (d) it's not illegal in Canada for emergency use.

2) The University of Toronto recently switched over to a Centrex III system. Certain (secretarial) phones can now display the number called and the number calling. The number calling works only if the call originated within the centrex exchange. It is not clear whether the restriction is technical or legal. The implication is that it's not illegal in Canada for calls originating within an enterprise.

It is clear that, if such a telephone were to become a consumer item, it would change the whole way we deal with telephones. I could refuse to answer calls from people I didn't want to speak to right now. In fact, I would probably program the micro in the telephone with a phone list of people who were and weren't allowed to disturb me. There would appear to be many human engineering problems to solve there. And many computer RISKS.

Michael

Re: Telephone switches

Bjorn Freeman-Benson <bnfb@beaver.cs.washington.edu>
Mon, 23 Mar 87 12:45:40 PST

>The issue of automatic callers releasing the phone line is actually
>a people issue rather than a technology issue.

As far as I know it depends on the "office" (telephone company term for switching equipment) connected to your phone. In the NW US there are three types: mechanical, ?, and electronic. A mechanical office will hold the line open as long as the caller has his/her phone off the hook regardless of the callee's actions. An electronic office will close the connection as soon as either party hangs up.

>Panic sets in and a feedback loop ensues.

However, I do agree that this can be a problem in any human system.

Bjorn N. Freeman-Benson

Re: ATM experience [Bruce McKenney, RISKS-4.66]

Roy Smith <cmcl2!phri!roy@seismo.CSS.GOV>
Mon, 23 Mar 87 21:31:56 EST

Clearly, different banks do things different ways. Some time ago I

wanted to make a mortgage payment at an ATM but couldn't find the right menu item. When I called for help, they told me to just pick any of the "deposit to ..." or "payment to ..." items. It seems that at least for the case of you making a deposit or payment, they totally ignore which button you pressed; it's what's on the slip that matters. In fact, it doesn't even matter which slip you use. They type of account is encoded in the account number. When I needed a "deposit to X" slip once and they didn't have any, I was told to just use a "deposit to Y" slip and write the proper account number on it.

The question is, doesn't this represent a real risk to the consumer (although, maybe not truly a computer-related risk)? I'm pretty ignorant of the ways of banks, but I've learned how my bank works. If I go to a different bank, I'm probably going to assume they work the same way, which probably means I'll get burned at some point.

Roy Smith, {allegra,cmcl2,philabs}!phri!roy
System Administrator, Public Health Research Institute
455 First Avenue, New York, NY 10016

Risks of ATM machines

Mike Linnig <LINNIG%ti-eg.csnet@RELAY.CS.NET>
Mon, 23 Mar 87 08:20 CDT

A year ago I happened on a remote gasoline station that allowed the customer to pay with an ATM card. After paying it occurred to me that this scenario was ripe for fraud.

How do I know that this ATM reader is really part of the ATM network?

Think about it...

First I let it read the bits off of my card and then I give it my secret PIN number. What is to stop some unscrupulous person from rigging a fake reader and duplicating my card (they already have my PIN number)?

Hmmm.. a few scandals like this and I bet we see smart cards with challenges and counter-challenges being exchanged between the card and the banking system.

Mike Linnig, Texas Instruments

[This is of course an example of the mutual suspicion problem that Mike Schroeder worked on in the 60s. Yes, you must trust the ATM apparatus, whether it is trustworthy or not. The same is true of any store that takes one of your credit cards, even with no computer in the loop. This is an old risk, but if RISKS never included discussions of old risks, our newer readers would be cheated. The safest solution is to avoid using such facilties, the next safest is to audit the records carefully. PGN]

Bank troubles, M.E. magazine

David Chase <rbbb@rice.edu>
Mon, 23 Mar 87 15:18:33 CST

Mechanical Engineering 2/1987 is the "What went wrong?" issue with articles on the Thresher and Chernobyl. Reading about Chernobyl makes me cringe. Again and again, "clear violation of operating procedures".

ME 2/1986 caught my eye with an article on space power and propulsion systems, but within it were articles on "The Dangers of CAD" [In the past, any discrepeancy between computer results and measured performance was traced down with an almost religious fervor. This zeal is still appropriate], human guided industrial "robots" (with some remarks on safety systems buried in there), and a study attempting to determine the safe speed for an emergency vehicle to enter an intersection (can the siren be heard?). Not all of these things are RISKS from computer systems, but I found it made interesting reading.

For bank troubles, I sent a check paying part of my bill to the insurance company, but they imprinted the entire amount on it for machine consumption (about 6 times more than the amount I intended). I actually figured this out before bouncing any checks because my account dipped rather surprisingly, but I spent a thin month trying to convince the bank or the insurance company that there might have been a mistake ("No, no, that couldn't have happened."). My bank rather quickly corrected my account when I showed them the cancelled check, but I'm sure it could happen again. You can be sure that I took my sweet time getting the rest of the money back to the insurance company. Of course, the source of this error was human, but it was compounded by blind faith in computers (and the efficiency of computerized check processing).

David

Re: "The Choking Doberman..."

Elliott S. Frank <amdahl!esf00@Sun.COM>
Mon, 23 Mar 87 14:16:21 PST

I've gotten some mail from risks subscribers requesting a citation for "The Choking Doberman...". Here's the citation from "Books in Print, 1986-1987" (courtesy the helpful folks at the Computer Literacy Bookstore):

> The Choking Doberman & Other "New" Urban Legends.
> Jan H. Brunvand, Norton, 1986, 256p. $6.95. ISBN 0-393-30321-7.

Elliott S Frank ...!{ihnp4,hplabs,amd,nsc}!amdahl!esf00 (408) 746-6384

Newspaper article on Audi 5000S

Mark Brader <msb@sq.com>
Mon, 23 Mar 87 18:30:56 EST

[This is a longish "summary", but serves a useful purpose in putting in perspective some of the previous messages on this subject. PGN]

Going through recent back issues of the Toronto Star, I found an article of about one full page about the Audi 5000S controversy, by the Star's automobile columnist Jim Kenzie. It was printed March 7, pages E1 and E15. At PGN's suggestion I supply a summary of the article's content.

* All the drivers interviewed on TV said the acceleration occurred upon shifting from P/N to D/R and that they had their foot hard on the brake.

* Paul Ast claims that failure of the idle stabilization valve can cause the engine to surge to 4000 rpm independent of the accelerator; William Rosenbluth claims that foreign matter in the transmission control valves can lead to a pressure buildup that pushes a rigid part of the throttle linkage that is only supposed to be pulled. These explanations conflict.

* Audi says there were no skid marks in any of the incidents, accelerator pedals were bent, they can't reproduce Ast's problem, and Rosenbluth's would involve severe transmission damage but the affected cars are new. Therefore they claim driver error and have recalled the cars to fit an interlock so you can't shift out of P without applying the brake.

* Kenzie (the columnist) revved an Audi 5000S up to 4000 rpm and put it into D while holding the accelerator steady. The car did not run away but took several seconds to reach 10 mph. There was also a lot of noise from the 4000 rpm idling, and a loud thump when the transmission engaged, which none of the victims apparently reported. So much for Ast's theory.

* Kenzie then pressed the brake and accelerator, all the way, simultaneously. The car revved up to 2700 rpm but stood still. Finally he took it up to 30 mph and did the same thing. It stopped. None of the victims, or their lawyers, has suggested a simultaneous temporary failure of braking, so it sure seems that Audi is right and the victims wrong. Probably they are simply repeating the same mental error they made originally.

* Some past Audis did have a minor unwanted-acceleration problem due to floor mats fouling the accelerator. Also, Audis used to have the brake and accelerator pedals close together and in the same plane so they could be "heel-and-toe" operated, but not since 1982 here, because most are sold with automatic transmission anyway. But these things could tend to make people more likely to blame the car when it is an Audi... a bandwagon effect. It is also possible that some "victims" are simply out for money in a class-action settlement.

* According to Tom Lankard of AutoWeek, the majority of Audis involved were newly bought, many by people switching from GM cars, which have the brake and accelerator much less close (so if you miss the brake you don't hit the accelerator). Many drivers were short, which would aggravate any confusion. [Does "many" mean "a statistically significant fraction"? --MSB]

* Kenzie doesn't know why the accidents only happen when starting from rest, but points out that once people are driving they already have their foot on a pedal and this provides a reference point. [He doesn't address at all the people who said they had BOTH feet on the brakes -- but at this point I'm willing to call them mistaken. --MSB]

The above is shortened about 80%. Kenzie's conclusion is worth giving in full:

> There is one party who DOES have guilt dripping from every pore, and that's television journalism. The 60 Minutes piece was shoddy in the extreme -- yellow journalism, in full color. They had convicted Audi before the show even began. Their story was grossly slanted, full of innuendo and witness-leading.
>
> The Today Show was only slightly better. They at least identified the prosecuting "experts" by name on screen, and had them explain how their theories worked. But Rosenbluth's credibility was destroyed when he "proved" how the Audi could accelerate due to hydraulic excess transmission pressure.
>
> First, without letting the audience know, he deliberately jammed both the normal pressure relief valves and the "fail-safe" backup ones in the car, which had been involved in two previous "incidents" and which still, for effect, had its left front fender missing.
>
> He tried to prove that it could happen -- not that it did happen. Second, he lightly brushed the brakes enough to turn the brake lights on for the camera, implying that the brakes couldn't stop the car from accelerating across the road into a ditch. He said he had to shut the engine off to stop the car. As I have previously noted, this is completely false.
>
> Only [the Canadian show] Market Place even attempted the tests that I did, which prove beyond a shadow of a doubt that the brakes will hold the car regardless of throttle opening. Still, they devoted about 10 seconds out of an eight minute piece to this vital fact.
>
> The public -- let alone Audi -- deserves better than this.

Search RISKS using swish-e

THE RISKS DIGEST

Forum on Risks to the Public in Computers and Related Systems

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

Volume 4: Issue 68

Thursday, 26 March 1987

Contents

Re: Health hazards associated with VDU use: eyestrain

Barry Gold <lcc.barry@CS.UCLA.EDU>
Wed, 25 Mar 87 17:13:43 PST

PGN's comment on the light spectrum from fluorescents ignored another "feature" of fluorescents: stroboscopic distortion. Take a small, bright object (like a pencil) and wave it back and forth under sunlight or incandescent light; you'll see a blur. Do that under flourescents and you'll see several copies of the object. Get the frequency right and you can even read the lettering on the pencil.

This means that movements (including the ones caused by your constant

eye motion) that would normally be smooth blurs (no feature to attract your auto-focus mechanism) work in jumps that can cause your eye muscles to try to track them.

An earlier posting on VDUs suggested keeping them at or above eye level. There is another good reason (besides neck strain) to do this. Our eyes were evolved for light coming from above. You'll notice your upper eyelashes are longer and thicker than the lower. And if you shave off your eyebrows and spend much time outdoors, you'll suffer eye damage (bet you thought eyebrows didn't have any function).

I keep my crt on an empty IBM PC box. This puts the bottom of the screen about level with my eyes. And most of the light--both from the screen phosphors and room light reflected off the screen--comes from above, as it should. I seem to be able to work more comfortably this way.

[Me too. Excellent advice. Thanks. PGN]

Risks of Displays and Fluorescents (Re: RISKS-4.67)

Brad Davis <b-davis@utah-cai>
Wed, 25 Mar 87 14:15:40 mst

[...] Or the 60 hz beat. I personally keep the window blinds open as long as possible since sunlight is better for stress and depression than most (read 'our') artificial lights.

Brad Davis {ihnp4, decvax, seismo}!cs.utah.edu!cai.utah.edu!b-davis

---

About CRT related injuries:

jeremy grodberg <rochester!kodak!grodberg@seismo.CSS.GOV>
26 Mar 87 22:23:44 GMT

Since I started working as a professional computer programmer, my eyesight has deteriorated from better than 20/20 to 20/60, with the bulk of that change (20/20 to 20/40 coming in the first 4 months). I have seen 3 different opthomologists who all agree my eysight degradation is due to excessive reading, but have been unable to stop the decay with glasses, excercise or drugs. I have now been at it 2 summers + 1 year since the first problems, and have little hope of reversing the damage even if I give up reading all together. While this injury is not necessarily related to CRT's, it is indicative of injuries that are occupational hazards with little hope of avoidance. My choice was to either lose (to some extent) my eyesight or switch to another profession. Until I am able to support myself some other way, I pretty much have to sacrifice my eyesight.

Jeremy Grodberg

Usenet: ...rochester!kodak!grodberg

Conference on Computers and Law

David G. Cantor <dgc@CS.UCLA.EDU>
Wed, 25 Mar 87 20:55:59 PST

IFIP CONFERENCE ON COMPUTERS AND LAW
A Technologist's Guide Through Legal Pitfalls and Pathways
October 21-23, 1987 at Santa Monica, California

Sponsors: IFIP Technical Committee On Computers and Society and
Los Angeles County Bar Association Law and Technology Section

WHO'S IN CHARGE:

Technology, law or the professional?

Technical and policy professionals are being forced to confront a maze of nascent legal realities and threats. These span private contracts, tort liability, the public interest, iminal prosecution, and myriad other issues and relationships, and encompass the regulation and protection of technology and data as derived from economic and political rights. Yet many problems are ill-defined and solutions are not widely recognized.

CONFERENCE AIMS:

To bring together computer and information professionals who must make technology-based decisions and lawyers who are faced with representing their interests in order to identify common problems, to explore the dimensions of their alternatives, and to understand the consequences of their responses.

SUGGESTED TOPICS:

Taxation and computing
Protection of intellectual property rights
Information-system imes and defenses
Legislative policy and technical issues
Telecommuting and independent contracting
Export-Import controls
Computer security---fact and fiction
Civil vs. criminal remedies: Victim options
Computer policy in developing nations
Government information policies
Database abuse: Public responsibility and private gain
Recognizing and minimizing exposure for product and service liability
International contracting for hardware, software, and computer services
Malpractice potential: Computer delivery of professional services
Resolving computer-contract disputes: Techniques and standards
Emerging technologies: Enyption, artificial intelligence, networks, and other problem areas
Public (dis-)service: Automating the criminal justice system
Independent verification and validation of computer generated information

Papers should strive to report important experiences and to identify key, open areas. We encourage tutorials for non-specialists, and presentations supported by check-lists and procedural guides. We also solicit panel-discussion proposals. Provocative comment is welcome.

HOW TO SUBMIT:

Original papers of up to 5000 words (20 double-spaced pages) are invited on the above and related topics. Papers which highlight actual user experiences, with specific legal entanglements or solutions, are preferred over abstract explorations. Papers will be refereed and accepted papers will be published in the Conference Proceedings. Format instructions for camera-ready copy will be provided when the paper is accepted. Please send FOUR copies of the paper, including a 300-500 word abstract, to the CONFERENCE CHAIR, Michael M. Krieger, P.O. Box 24619, Los Angeles, CA 90024, 213-394-4356, Internet: complaw@math.ucla.edu

IMPORTANT DATES:

Papers due: May 6, 1987 Acceptance: June 5, 1987 Final copy due: July 15, 1987

ORGANIZING COMMITTEE: Jay BloomBecker, Los Angeles (program chair),
Richard Bernacchi, Los Angeles David G. Cantor, Malibu
Steve ocker, Los Angeles Eric Delissy, Geneva
Charles Firestone, Los Angeles Jochen Haber, Los Angeles
John Helly, Los Angeles Richard Horning, San Franscisco
Leonard Kleinrock, Los Angeles Dr. Wolfgang Kilian, Hanover
John Lautsch, Anaheim Ira D. Moskatel, Beverly Hills
T. R. H. Sizer, Farborough Dr. Artur Solarz, Stockholm
Wilhelm Steinmuller, Bremen Alan S. Wernick, Columbus
David C. Tunick, Los Angeles (proceedings editor)

Re: runaway motors [and a fish tale?]

<LINDSAY@TL-20B.ARPA>
Wed 25 Mar 87 10:58:44-EST

Theatrical riggers are not the only people in the world with computer-controlled motors.

Some friends of mine set a good example when they retrofitted computer controls onto a mechanical stereo-interpreter. This machine is used to make topographical maps from aerial photographs ("stereo pairs", hence, "stereo-interpreter").

The machine had a mechanical stage, with arms driven by ultra-precise worm gears. The stage had mechanical stops - that is, solid objects which the arms would have to run into before leaping onto the floor. My friends changed the drive, of course, and the resulting machine was quite fast. I recall seeing the arms travel six feet in under a second. (This includes decelerating

to a stop.)

The machine acquired several layers of computer equipment. At the low level, there was a microprocessor per motor, and detection hardware so that precision could be obtained by feedback. At the higher level, of course, one made maps.

The design incorporated simple limit switches. These switches tripped when the arms got out of bounds, and shut off the power to the motors. The basic idea was to keep the arms from hitting the mechanical stops at high speed. This would prevent damage to the arms, and also, would prevent then from bouncing over the stops and onto the floor.

The wise thing that my friends did, was to install the limit switches FIRST. The computer interface to the limit switches was added LAST.

In the course of the project, it was noticed that there was a single major failure mode. The arms would go past the limit switches at maximum acceleration. This was the result of practically anything - timing glitches, byte-ordering bugs between machines, reading a device register while it was rippling, you name it.

I heard a related story from a friend working on irradiation therapy machines. He reported that an older machine of theirs was once involved in an tragedy. Reportedly, a patient had been killed because the hydraulics ran away, and crushed the patient against the radiation shielding. The operator had hit the emergency-off switch, AND IT DIDN'T WORK. The switch removed power from most of the machine - but not from the hydraulics.

And then, there is the story that I heard about a real-time programmer who was computerizing a fish-filleting factory. As I heard it, a side effect of debugging was that he got to feed every stray cat in Stockholm ...

Don Lindsay

[This is known as REEL-TIME Programming. Must have been "Salmon-Chanted Evening" for the cats. PGN]

---

the social implications of inadvertent broadcasts

Donn Seeley <donn@utah-cs.arpa>
Thu, 26 Mar 87 02:31:36 MST

[This is somewhat marginally relevant, but it seemed worth including anyway. PGN]

I happened upon this in the New York Times (3/21/87, p. 12). '... [I]n February, The China Daily reported this week, ... a woman trying to copy an obscene film called "Massage Girl" at a television station inadvertently broadcast 20 minutes of the movie to homes throughout Guangdong Province. The woman was arrested.'

I live in a state where the attorney general's office has spent $600,000 in public funds to appeal a ruling that the legislature's

cable TV censorship law is unconstitutional, and where a local newspaper that has recently stopped printing the controversial comic strip Doonesbury is now debating whether to continue to buy the strip and not publish it so that the population at large need not suffer from its presence. An 'inadvertent broadcast' like the one described above could have a serious impact on civil liberties here, especially if it occurred on a cable channel.

Donn Seeley University of Utah CS Dept donn@cs.utah.edu

Re: Increased Telephone Switching Capabilities

Andrew Klossner <andrew%lemming.gwd.tek.com@RELAY.CS.NET>
Wed, 25 Mar 87 15:08:58 PST

This topic was discussed at length in the TELECOM list. Some items ...

> "I discussed this article with a friend, who [asserted that] the information (calling #) is already available, and is encoded somehow just prior to the ring spike on the receiving line."

There is no truth to this statement. Under normal circumstances, when the originating and receiving exchanges (CO's) are different, the receiving exchange has no way of knowing the origination number.

> "I don't see any obvious risks to the new features."

On of my concerns is that, with these features, I can no longer keep my unlisted phone number private. If I call a local department store to get their price on a pair of shoes, I may start getting unsolicited shoe sales calls from all over. Merchants would be motivated to collect and sell lists of phone numbers of consumers with particular interests, just as they now collect and sell mailing addresses. (And I can't make use of that "call screening" feature; what if my daughter is in trouble and tries to call home from a phone booth?)

MORE: Re: Michael Wagner (RISKS-4.67)

> "1) the 911 emergency number in Toronto displays the number from which a call was made...

An originating exchange sends the information only when it's using the special 911 subsystem. (At my exchange this goes out on a special trunk directly to the 911 center, it doesn't travel between exchanges.) The implications don't follow.

> "2) The University of Toronto recently switched over to a Centrex III system. Certain (secretarial) phones can now display the number called and the number calling. The number calling works only if the call originated within the centrex exchange. It is not clear whether the restriction is technical or legal...

It's technical, that's the Centrex system talking to itself.

-=- Andrew Klossner (decvax!tektronix!tekecs!andrew) [UUCP]
(tekecs!andrew.tektronix@csnet-relay) [ARPA]

Re: phone number of caller

<LINDSAY@TL-20B.ARPA>
Wed 25 Mar 87 11:19:30-EST

At first glance, it seems simple to be told where your caller is calling from. All that one needs is a small display: after all, exchanges are computerized now, aren't they ?

Well, yes, new ones are. Also, new exchanges tend to be bigger: several exchange numbers are implemented by a single office, rather than being one-for-one. And, of course, if all the action occurs within a single exchange, then the features that are offered are just a Small Matter Of Programming.

However, old phone exchanges are still with us. Projected reliability used to be stated as outage-time per forty years ! Also, old designs were being built until recently. For example, Bermuda bought a mechanical stepping exchange (from Philips) in the early 1970's.

When authorities try to trace phone calls, the major stumbling block is usually that the call has crossed one or more boundaries between exchanges. Tracing then becomes a serial process, and it used to involve a human at each physical location. A person wishing to (say) utter death threats was quite difficult to catch, particularly if rural equipment was in the chain.

Of course, we will eventually resolve these problems. Mad bombers will respond by using pay phones, unattended autodialers, and other tactics.

Don Lindsay

Who called? (Re: RISKS DIGEST 4.66 and 4.67)

jeremy grodberg <rochester!kodak!grodberg@seismo.CSS.GOV>
26 Mar 87 22:58:37 GMT

According to _High Technology_, a caller placing a call from an unlisted phone can prevent the number from being displayed on the destination phone by entering a code. The phone company equipment still gets the number though, so the person being called can call still call the person with the unlisted phone number (using a feature which dials the number of the most recent incoming call), although there is no (legitimate) way to actually determine the unlisted number.

Jeremy Grodberg

Hang-ups [Re: RISKS-4.67]

Paul Wilcox-Baker <dual!paul@ucbvax.Berkeley.EDU>
Wed, 25 Mar 87 09:24:37 pst

> As far as I know it depends on the "office" (telephone company term for
> switching equipment) connected to your phone... An electronic office will
> close the connection as soon as either party hangs up.

Actually, this is not true. For most electronic exchanges in the U.S., the connection is held until about 20 seconds after the called party hangs up, or whenever the calling party hangs up. This is supposed to let the answering party hang up one phone, move to a different room and continue using another. The timeout is reset every time the phone goes off-hook. This causes the apparent inability to get rid of the incoming call. The best solution to obnoxious electronic calling machines is legal - ban the damn things!

Paul Wilcox-Baker.

Search RISKS using swish-e

THE RISKS DIGEST

Forum on Risks to the Public in Computers and Related Systems

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

Volume 4: Issue 69

Friday, 27 March 1987

Contents

Cellular phone fraud busts

the tty of Geoffrey S. Goodfellow <Geoff@CSL.SRI.COM>
Fri 27 Mar 87 08:22:15-PST

18 Arrested for Altering Their Mobile Phones
By LEONARD BUDER, c.1987 N.Y. Times News Service

NEW YORK - In a federal attack on a crime made possible by the latest technology, 18 New Yorkers were arrested Thursday on charges of using illegally altered memory chips in their mobile telephones so they could make calls without being charged for them.

Also arrested were seven others who, the authorities said, illegally reprogrammed the chips and placed them in the mobile telephones. Such telephones can be installed in vehicles or carried by individuals.

It was the first time anyone in the country had been arrested for this kind of crime involving cellular telephones, said Thomas L. Sheer, the assistant director of the Federal Bureau of Investigation who is in charge of the New York office.

He said the problem of fraud in the cellular telephone industry had grown significantly in the last six months and that Thursday's arrests were the result of ''the first of a series of initiatives'' being

undertaken by the bureau and the Secret Service to counter fraud in emerging technologies.

''Every new technology carries with it an opportunity to invent a new crime,'' said Laurence A. Urgenson, the chief assistant U.S. attorney for the Eastern District of New York.

The first commercial cellular mobile telephone service began late in 1983. According to the Cellular Telecommunications Industry Association, there were nearly 682,000 customers of such phone services at the end of last year.

Sheer said the government was making ''aggressive use'' of a federal statute dealing with ''Fraud in Connection with Access Devices,'' that was originally intended to combat credit card fraud but is now being interpreted to cover frauds involving all computer-based or computer-assisted systems. [...]

The 18 people who had the illegally altered chips installed ''awoke this morning to find that their cellular telephones had been disconnected'' electronically, Sheer said at a news conference held at the bureau office at 26 Federal Plaza in lower Manhattan.

''They're going to get one phone call today,'' the FBI official added - referring to the call a person is permitted to make after being arrested - ''but it's not going through from a cellular telephone.''

The officials said the arrests followed a six-month investigation that involved the use of a confidential informer who installed the chip and federal agents working under cover. The authorities acknowledged the cooperation of the Nynex Mobile Communications Co. in the investigation. Sheer said the investigation was assisted by ''recent technological advances in computerized telephone-switching equipment and billing systems.'' [NB!!]

Sheer said that the fraud, which was not the product of an organized conspiracy, cost local mobile telephone companies about $40,000 a month and that nationwide, carriers of cellular services were losing about $3 million a year because of frauds.

The authorities gave no details about the alteration of the chips. [...] The most serious charge that could be brought against each carries a maximum term of 10 years in prison and a possible fine of $250,000.

Sheer said the installers usually charged $500 to reprogram and install two memory chips in a cellular phone. The chips, in their unaltered state, are sold in computer equipment stores at a price of two for 89 cents, an FBI agent said.

According to the federal authorities, each cellular mobile telephone has a memory chip containing a mobile identification number, or M.I.N., and another containing an electronic serial number, or E.S.N. When a mobile telephone call is made, the two numbers are automatically transmitted to the mobile carrier.

The mobile carriers make a computer check of the E.S.N. to see if it is valid. If it is, the call goes through and the cost is billed to the billing number provided by the M.I.N. chip.

By using illegally reprogrammed chips, the federal complaint said, other people were billed for calls made by those participating in the fraud. [...]

<minow%thundr.DEC@src.DEC.COM>
Fri, 27 Mar 87 06:30:39 PST

(Martin Minow THUNDR::MINOW ML3-5/U26 223-9922 27-Mar-1987 0916)
To: "risks@csl.sri.com"@src.DEC.COM
Subject: "... and its fate is still unlearned..."; robotic exploration of Mars

From a Boston Globe editorial, 27 Mar 1987, on the local subway system:

> Of the MBTA's four lines, only the Orange Line trains now run consistently on time. In fact, the Orange Line has one of the best on-time records in the nation -- a record that some of the line's old-timers fear will be lost when the antique manual-switching equipment is replaced by computerized signals later this spring.

On the same issue's op-ed page, M. R. Montgomery writes about a geophysicist's proposal for robotic exploration of Mars:

> The lowest estimate for getting a robot to Mars and back is $10 billion, and if you wonder why it's a nice round number, it's because the real cost is an unknown double-digit billion -- and 10 is the lowest one you can float, even in front of a Mars-starved country.
>
> ... A lot of tiresome hogwash being floated about the benefits of robotic exploration of Mars, of which the worst is the assertion that the way to make advances in human-serving robots is to build one whose main function is to go 50 million miles to pick up dirt.
> ... If you wanted to benefit mankind by improving robotic science, you should start out with something really complicated, not something trivial that is only expensive because it's happening 50 million miles away. You could build a seeing-eye dog robot that understood the difference between First Street and First Avenue, between the inbound streetcar and the outbound cars, and never, ever, had to go to the bathroom.
>
> But that would mean spending $10 billion on the visually handicapped, which is not nearly as much fun as spending it on athletic men and women in silver suits, and, all in all, even less enjoyable than spending it on our geophysicists.

Re: Returned mail -- "Host unknown"

Richard Schedler <schedler@src.DEC.COM>
Fri, 27 Mar 87 11:32:03 PST

> [RISKS received a bunch of Host-Unknown BARF messages from DEC. This is the reply I got from Richard when I reported the problem. PGN]

The addresses are valid. It just happened that our DECnet node database was being updated at the time the messages were being processed. Due to the size or our database (~173 Kbytes) we have a window of vulnerability around 1:45am each night where some nodes won't be defined.

[My reply noted that since Les Lamport now works for DEC SRC, SRC should have found a way to avoid this problem. Perhaps their software was written by a Byzan-tine-ager. (I continue to receive many messages each day resulting from idiosyncratic net software; I really wish it were more robust. I am not looking forward to the 1 April cutover.) PGN]

Re: Phone problems (RISKs in auto-dialers)

Larry E. Kollar <ucbcad!ames!seismo!gatech!dcatla!mclek@ucbvax.Berkeley.EDU>
Wed, 25 Mar 87 09:00:46 EST

In RISKS 4.63 David Barto writes about experiences with auto-dialers, then asks:

> >Could this become a major RISK in the future, dialing wrong numbers
> >for hours on end?

Scott Watson, the author of the Red Ryder terminal communications program for the Mac, describes just what can happen when you turn an autodialer loose on the world without making sure you're dialing the right number. (From the Red Ryder 8.0 manual, by Scott Watson, reprinted without permission.)

> "When I used to operate a BBS in my home, it had the bad habit of crashing every day or two.... It was easy to tell when the BBS crashed, because some jerk would then decide to start redialing my voice line (just to see if there was a BBS connected _there_, I suppose). Of course, he turned off his modem speaker... and therefore couldn't hear me screaming "Hullo?" (or much worse).... One night, I got _very_ angry and answered the phone - twice per minute - for over three hours. I suspect he got the message when his phone bill arrived the next month - I hope he was calling from Boise."

If your modem doesn't have a speaker, (or doesn't respond "NO CARRIER") you can listen in on a cheap phone plugged into the appropriate jack to make sure you typed your number in right. Look before you leap.

Re: ATM experience [Bruce McKenney, RISKS-4.66]

Brent Chapman <chapman%mica.Berkeley.EDU@BERKELEY.EDU>
Thu, 26 Mar 87 23:14:35 PST

It actually gets worse. It turns out that many (most?) banks ignore (or at least _used_ to ignore; hopefully they've learned, but I wouldn't bet on it) what's _written_ on the check/deposit stub/whatever if that field is already encoded in the magnetic character information at the bottom. For example, if there's already a "from" account encoded there, the operator isn't ask to enter one.

Well, there's a slight bug in that system... What happens if someone goes into a bank branch, walks out with a stack of the blank "courtesy" deposit slips, takes them to a "shady" printer who encodes the person's account into the "to" field at the bottom of the form, and then replaces the forms in the

bins in the bank. Eventually (within a few days, usually) this will get noticed, but assuming that all the doctored forms get used within a single day, and that many (most?) of the deposits falsely credited to the crook's account clear within a day or two, one could drop of the forms one day, and withdraw a substantial amount of cash a day or two later...

Now, some banks have dealt with this by not offering the "courtesy" forms any more. Others have presumeably (hopefully!) dealt with it in other ways, with which I'm not familiar. But I wouldn't be surprised if this scam would still work with a significant number (5 or 10%? Even 1% would be useful, if one knew which 1%...) of banks...

Comments? Is my information out of date? I have an aunt who is a teller for First Interstate Bank (side comment: isn't "FIB" a _wonderful_ acronym for a bank? :-), who told me some of this stuff, and I got other parts of it from several different books on electronic security (unfortunately, I don't remember the titles or authors of any of them..).

Brent Chapman chapman@mica.berkeley.edu or ucbvax!mica!chapman

Search RISKS using swish-e

THE RISKS DIGEST

Forum on Risks to the Public in Computers and Related Systems

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

Volume 4: Issue 70

Wednesday, 1 April 1987

Contents

Rocket Shot Down By Faulty ``Star Wars'' Weapon (From the AP wire)

Phil R. Karn <karn@flash.bellcore.com>
Wed, 1 Apr 87 19:34:50 est

AM-RocketFailure-StarWars 04-01 0400
AM-Star Wars,400
Rocket Shot Down By Faulty ``Star Wars'' Weapon
By Lou Flirpa
Associated Press Writer

WASHINGTON (AP) _ Reliable Pentagon sources have reported that last Thursday's explosion of a $78 million Atlas-Centaur rocket carrying the $83 million military ``FltSatCOM'' communications satellite was in fact caused by a ``minor malfunction'' in a highly secret experimental Strategic Defense Initiative beam weapon, commonly known as ``Star Wars''.

``We're not sure yet what happened'' said one highly placed source, who spoke on condition that he not be identified. ``But we think the autonomous boost-phase battle station we launched on Delta last year mistook the Atlas for a Soviet ICBM and shot it down. Naturally we all feel pretty bad about this. Gosh, we're real sorry. Really.''

Speculation had been mounting after the launch failure that the Atlas had been hit by lightning. According to sources, however, ``a charged particle beam weapon is essentially an artificial lightning machine.''

Since the launch took place in a rainstorm, it was easy to jump to the conclusion that lightning struck the vehicle, the sources said, especially since no one actually saw the explosion because of the cloud cover.

While the exact cause of the ``malfunction'' has not yet been determined, there is early speculation that the on-board ``clock'' of the battle station was incorrectly set five hours ahead of ``universal'' time instead of five hours behind, leading it to ``believe'' it was over the Soviet Union when it was really over Florida.

``It looks like some of our scientists got confused over which way the earth turns. I guess they found out the hard way,'' said another source.

SDI director Lt. General James A. Abrahamson was reported to have ``mixed feelings'' when told of the accident.

AP-NR-04-01-87 1313EST

ATMs, phones, health hazards, and other sundry subjects

Peter G. Neumann <Neumann@CSL.SRI.COM>
Wed 1 Apr 87 22:29:27-PST

In the epicycles of RISKS, I think we are ebbing. 12 recent messages to RISKS were slight variants on earlier ones, and I have decided (of course, very arbitarily) to blow the whistle. Sorry to those of you who composed careful messages that are not included in this issue.

I conducted a few informal polls, and feel (at this point in RISKS) that I have been too permissive lately, and have even lost a few readers who cannot devote the time to screening (literally). Thus (for a while, at least), I will try to include only the more incisive contributions. (You may notice that I try to put the more exciting things FIRST -- unless they are very long, in which case I tend to put them LAST.) On the other hand, fear not for withdrawal symptoms -- some new disaster always tends to happen, and we are off again in another direction...

By the way, there was this response to my earlier note on this metasubject:

> From: AGRE%OZ.AI.MIT.EDU@XX.LCS.MIT.EDU
>
> I'd like it to enter the culture that whenever someone runs into an incredibly obscure bug, they feel a sense of responsibility to share it with the community, to save others the same hassle and danger. RISKS could become the customary channel for this.

Following are a few messages that I let slip by.

Computer Risks in Theatre (Re: RISKS-4.68)

Warwick Bolam <munnari!goanna.oz!wjb@seismo.CSS.GOV>
Mon, 30 Mar 87 10:45:03 EST

Recently, a stagehand was severely injured in a Melbourne theatre. He was on a stage-ladder. These are large, free-standing ladders that are wheeled from place to place on the stage to facilitate access to the grid area above the stage. The ladders are massive, very stable and hydraulically operated. The accident occurred when someone activated the computerised stage moving system. This system allows sections of the stage to be raised, lowered and moved about. The ladder was at the front of the stage, the parts of the stage that were intended to be moved were at the rear. A mistake was made and one of the sections that the ladder was standing on was moved. The ladder toppled and the stagehand suffered a fractured skull and a broken pelvis. It was fortunate that no one else was hurt. Standing orders are not to move the stage when there are people on it, but this is commonly ignored.

Warwick Bolam wjb@goanna.oz

PC fumes

Dick King <king@kestrel.ARPA>
Mon, 30 Mar 87 13:48:41 pst

> From: vortex!lauren@rand-unix.ARPA (Lauren Weinstein)
> Subject: Fumes from PC's
> The most likely cause of a problem is OZONE..

Induction motors don't generate ozone, and those are the type used in computer fans and [probably] disks. A more likely source of ozone is the CRT high voltage.

There may be other sources of fumes in a PC, such as undried solvent -- does anyone know anything about this?

A real eye-catching headline

David Chase <rbbb@rice.edu>
Sat, 28 Mar 87 02:25:20 CST

IEEE Spectrum, April 1987:

"Inherently safe nuclear reactors"

[Add to the oxymoron list. PGN]

Risks of being fuzzy-minded

<TMPLee@DOCKMASTER.ARPA>
Mon, 30 Mar 87 17:43 EST

All right, already. My pilot ("Overconfidence in Airplane Computers") was more right than I: the thrust of the plane IS measured in the same kind of units as its weight, and to say that one is half of the other is a meaningful statement (the plane takes off with half the acceleration it would have if it were dropped off a cliff). My only defense is that as a defrocked physicist I'm so used to people getting mass and weight confused that I automatically assumed it had happened one more time. The letters can stop.

<ihnp4!wlbr!gins@ucbvax.Berkeley.EDU>
Sat, 28 Mar 87 08:40:00 PST

Deposits on ATM:

Various banks have various systems. As an example, at CITIbank a deposit was made to a specific account. Your account was updated with a MEMO update, i.e. it would show up on your balance. However it did not become AVAILABLE funds until it was verified by a teller. On the envelope was Customer ID number, the envelope number and the Entered dollar amount, the branch # and the Machine #.

There was also a selection for OTHER PAYMENTS. This allowed you to dump any deposit into the ATM.

What are you assured then when you deposit to an ATM ?

1) You have a banking RECORD (not a reciept at Citibank). If you have this record, there is a VERY high percentage that you deposited something at that ATM.

2) Some banks have ways of crediting your deposit RIGHT NOW. This could be done by a balance in another account (i.e. a long term C.D. or a line of credit.) That way they can get you if you lied.

ATM Splitting a Card in half

I've worked with about 75% of the types of machines on the market and NONE of them split a card in half upon swallow. However, some NETWORKS have a policy of slicing a card to avoid security problems.

Trusting an ATM.

Interesting you should bring this up, I'm just bruising up a paper describing a REAL situation where your card and PIN are in the clear. This involves a customer using a bank that is part of a network. All the information was available to folks in DP, if they put in some

efforts to get it.

Re: ATM experience ... it actually gets worse [Chapman 1987 03 26]

Allen Brown <brown@dreo-ewd.arpa>
Tue, 31 Mar 87 15:21:54 est

[Included for the reference. Perhaps it will stave off further repetition.]

Brent Chapman makes reference to magnetically encoded deposit slips, and the interesting differences between human and machine interpretation of the same piece of paper.

In one story, a customer surreptitiously laid out courtesy slips on the bank counters which had been magnetically encoded with his account number. It ended in the customer's withdrawal of $100K of others' money and his subsequent disappearance. Such actions have, apparently, taken place in several banks.

In another case, a cheque had been magnetically encoded with a valid bank branch code (and a bogus account number) that was different from the name of the bank on the cheque paper. The perpetrator had originally deposited a large sum of money in the bank indicated on the cheque paper. Then he opened bank accounts in a number of other banks using these cheques. Owing to machine-sorting each cheque bounced back and forth between two banks, with an associated transit time of two days per rebound. The machine at one end could not validate the account and hence dumped it into a pool for manual sorting, where the human response was to assume a simple routing error (because the bank name on the cheque was certainly not theirs), at which point it was sent to the named bank. At the named bank the cheque was machine-sorted for final clearance, and since it was coded for another bank (the first one), it was automatically directed (back) there. The hoax was only discovered because the well-travelled cheque became too frayed by machine handling to be further automatically processed. Having had a number of such cheques accepted for deposit, the depositor had made withdrawals and had disappeared with $1M by the time of discovery.

These stories, and a number of others are recounted in a ``delightful'' little book called Computer Capers (Mentor, 1978 - no ISBN) by Thomas Whiteside. Most of the material appeared originally in The New Yorker. Whiteside has a good bibliography for titles published between 1966 - 1977, but the book is clearly now a bit dated. White-collar crimes have undoubtedly advanced beyond the ``stone tools and knives'' stage of ten years ago, but you can be sure that we won't hear about them from the banks, etc.

Allen Brown

Report problems with the web pages to the maintainer

Search RISKS using swish-e

THE RISKS DIGEST

Forum on Risks to the Public in Computers and Related Systems

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

Volume 4: Issue 71

Sunday, 5 April 1987

Contents

Re: A real eye-catching headline [David Chase, RISKS-4.70]

Jerome H. Saltzer <Saltzer@ATHENA.MIT.EDU>
Fri, 3 Apr 87 17:49:56 EST

> "Inherently safe nuclear reactors"
> [Add to the oxymoron list. PGN]

Before assuming nonsense, one might try reading the article under the headline. It explores a series of design approaches with the common theme that safety mechanisms should be driven by simple, passive, inexorable laws of physics rather than being complex gadgetry in themselves. (For example, place the entire reactor system under water so that faults that would usually produce loss-of-coolant failures tend to instead produce too-much-coolant failures.)

Whether or not the specific technical ideas are competent I can't judge, but the notion of designing safety measures that are simple and inevitable seems something that people concerned with computer RISKS should want to ponder rather than laugh at.

Jerry

Re: A real eye-catching headline

<Peter G. Neumann <Neumann@CSL.SRI.COM> [Edited]>
Fri 3 Apr 87 16:55:55-PST

Yes, indeed, I certainly agree that one should understand something well enough before making light of it. In fact, the IEEE Spectrum article is quite significant. Use of inexorable laws of physics is a marvelous idea -- if those laws are in fact complete, correctly understood, immutable, and nonbypassable... The principle is excellent in the small. The practice may not be so easy to guarantee in the large. [See also Henry Spencer's message below.]

I would like to add something that addresses not the inexorability, but rather the limitations of the environment in the case of large-scale nuclear power (to which this technique has not yet been applied):

1. People are not infallible, and are certainly not "inherently safe". Incompent or careless people might make an "inherently safe" nuclear reactor ACTUALLY UNSAFE. PBS' All Things Considered on 3 Apr 87 concluded that BAD MANAGEMENT was probably the biggest source of problems. Bad management is quite capable of rendering a system inherently unsafe, e.g., as a result of unwise cost-saving measures. (Philadelphia's Peach Bottom plant was just closed by the NRC; a surprise visit found the operators sleeping on the night shift. The PBS program also noted a safety system installed backwards.)

2. The inexorable laws (in the small) may be circumvented under actual environmental conditions, i.e., to the system in-the-large -- via accidents, sabotage, earthquakes, carelessness, and improper maintenance, as well as bad management and other human behavior noted above.

[3. Despite claims to the contrary, nuclear waste disposal appears to be at least LONG-TERM RISKY, and may prove to be INHERENTLY UNSAFE. There appear to be no really appealing solutions in the long run, but that argument is beyond the scope of RISKS. I toss it in simply to illustrate the holistic nature of the problem and the nonholistic nature of the assumptions of infallibility.]

It does seem that assumptions are being made about the INFALLIBILITY of the technology. I quote from the Spectrum article:

> "If a major system fails, for example, the core is flooded automatically with coolant that flows under immutable laws of gravity and thermohydraulics, not under propulsion by mechanical pumps and electromagnetic actuators."

If applied to nuclear power, does this ignore all sorts of fallibilities? Are there not still combinations of mechanisms and components that might fail, e.g., if the coolant suddenly springs a major leak, or if during maintenance reliance on the "INHERENTLY SAFE" physical principles must temporarily be circumvented, or if people do not always behave reasonably, as assumed? The notion that it is possible to design something that is "100% reliable" UNDER ALL POSSIBLE CIRCUMSTANCES is clearly unrealistic.

But, even "99.9999% reliable" is not very good if the .0001% case can be provoked accidentally or intentionally by a specific combination of plausible circumstances (whether anticipated or unanticipated). Of course, A VERY REAL RISK LIES IN BELIEVING IN THE INFALLIBILITY OF TECHNOLOGY.

Nevertheless, the cited April 87 IEEE Spectrum article is worth reading, and Jerry's points are very well taken. For those technologies in which risks can be substantially reduced by using homeostatic processes, that should be encouraged. (Although nuclear power has not yet been so based, the article makes an important point that it should be!) A good example of homeostasis is the human body, which is basically self-regulating -- except that when it breaks down, all bets are off.

(To the reader: I know that Jerry doesn't believe in the infallibility of technology. I am not trying to shoot a straw herring in the foot. This message is by way of further discussion.)
Peter

Re: A real eye-catching headline

<pyramid!utzoo!henry@hplabs.HP.COM>
Sun, 5 Apr 87 16:46:06 pst

> IEEE Spectrum, April 1987:
> "Inherently safe nuclear reactors"
> [Add to the oxymoron list. PGN]

Not so, actually. The things actually exist, and the term accurately describes them. You could take a sledgehammer to the controls and nothing much would happen. U of T has one. Apparently if you're the last one to use it Friday afternoon, you just lock the door behind you and leave it unattended for the weekend. Unlike power reactors, the design is inherently stable: an increase in temperature causes a decrease in reaction rate, so nothing you can do will make it overheat. Unfortunately, the design does not scale up well and hence isn't useful for power plants.

Henry Spencer @ U of Toronto Zoology {allegra,ihnp4,decvax,pyramid}!utzoo!henry

[The Spectrum article suggests that it COULD be useful for power plants... PGN]

A non-fail-safe ATM failure [Still one more interesting ATM saga!]

Don Chiasson <CHIASSON@DREA-XX.ARPA>
Thu 2 Apr 87 08:38:46-AST

I'd like to pass along one which happened to me and indicates the risk of interactions between computers and mechanical components in automated systems. A few months ago I used an ATM to pay a bill. At the end of the transaction, the machine said to:
"REMOVE CARD TO QUIT OR PRESS OK TO CONTINUE".
I was done, so I pulled out my card and started to leave. I took a few

moments getting my credit card back in my wallet, then had one of those "What wasn't that??" feelings. The door on the ATM hadn't gone down. The mechanical switch which shows whether my card is or is not in the machine had stuck and the ATM was patiently waiting for my next transaction. I aborted it by pressing a "CANCEL" button. Had I not done that, anyone passing by (this machine was outdoors) could have pressed a few buttons and paid their own bills from my account or pulled out my daily cash limit.
Lesson: verify that the machine is doing its thing.

Don

[Despite a RISKS moratorium on routine ATM stories, this one is worth including as an example of an uncompleted supposedly atomic transaction with nasty side-effects. Another example of inconsistency between the state of the software and the state of the hardware was the THERAC 25 therapeutic radiation device: you recall that the software thought it had switched the device to X-ray mode (1,000 rads), but the device was still in electron-beam mode (up to 25,000 rads) at the moment.
(See RISKS-3.9.) PGN]

Fumes from computers and other electronic appliances

Richard Thomsen <rgt@LANL.ARPA>
Thu, 2 Apr 87 07:33:33 mst

Just as radon gas comes from cement walls and formaldehyde comes out of new housing walls, carpets, and some modular furniture, there are gases that are emitted from electronic appliances. I do not know what they are, but suspect they come from the plastic cases, and probably the circuit boards and capacitors.

I know someone who is highly allergic to chemicals, and can smell these gases. They are more prone to be emitted when the computer is on, since it is warmer.

[This subject needs some real expert contributions. PGN]

Open University Fire

"Lindsay F. Marshall" <lindsay%kelpie.newcastle.ac.uk@Cs.Ucl.AC.UK>
Sun, 5 Apr 87 11:29:51 gmt

Recently there has been considerable publicity given to a fire that took place in a computer room at the Open University HQ. The fire destroyed a VAX and all its back-up tapes that were stored in the machine room. The interesting thing about this event was the various reports of the problems caused by the loss of the filestore back-up. Initial (non-trade) press reports talked about people losing 15-20 years of research, this was then whittled down to two to three years (in the trade papers) and eventually seems to have come down to a couple of months as most people had personal back-ups of critical data!!

Lindsay F. Marshall, Computing Lab., U of Newcastle upon Tyne, Tyne & Wear, UK

Search RISKS using swish-e

THE RISKS DIGEST

Forum on Risks to the Public in Computers and Related Systems

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

Volume 4: Issue 72

Wednesday, 8 April 1987

Contents

New kind of computer-technology-related deaths?

Peter G. Neumann <Neumann@CSL.SRI.COM>
Tue 7 Apr 87 23:36:22-PDT

Some strange recent events in England seem computer- and defense-system related, although in a diffuse and rather mysterious way. At this point any commonality among 6 different cases must be considered speculative. However, the "pure coincidence" explanation is not too satisfying, and certainly whets the appetites of conspiracy or collaboration theorists. The following is reported here for the RISKS record, awaiting any further clarification.

August 1986: Vimal Dajibhai, 24, programmer with Marconi Underwater Systems, reportedly working on Britain's self-guided torpedo Stingray missile. Found dead beneath a suspension bridge. (No cause identified.)

October 1986: Ashad Sharif, 26, computer expert with Marconi Defense Systems, bizarre death, seemingly suicide.

January 1987: Richard Pugh, computer design expert, found dead in his home.

January 1987: Avtar Singh-Gida, 26, disappeared in northern England while conducting experiments on submarine warfare equipment.

22 February 1987: Peter Peapell, 46, metallurgist involved in secret defense work, died of carbon monoxide poisoning. (Wife doubted it was suicide.)

30 March 1987: David Sands, 37, computer expert working for a Marconi subsidiary on an air force defense system, killed when car crashed into cafe.

The British government claims there is no evidence linking the cases. However, Home Secretary Douglas Hurd has ordered police involved in these cases to contact each other. [Source: SF Chronicle, 6 April 1987]

Conrail Sale Funds Transfer

<Chuck.Weinstock@sei.cmu.edu>
6 Apr 1987 20:18-EST

From Business Week, April 13, 1987:

The sale of Consolidated Rail Corp. almost blew some fuses at the Treasury Dept. Because Treasury's computers can only handle single transactions of up to $1 billion, underwriters had to break the $1.6 billion from the public offering into two parts before electronically transferring the funds to the government. The underwriters, led by Goldman, Sachs & Co., got a nice chunk of change sent their way too -- $70 million in fees.

[I'm surprised that someone was smart enough to know about the $1 billion problem before it really did "blow a fuse". Who knows where the $600,000 million might have ended up!]

Re: "Inherently safe nuclear reactors" (RISKS-4.71)

Phil Ngai <amdcad!phil@decwrl.DEC.COM>
Mon, 6 Apr 87 08:44:03 PST

If I understand correctly, such principles are used outside of the lab. According to two books I have read (_The Hunt for Red October_, and _Submarines_), all American subs and many Russian subs operate the same way. When you draw more power out, the coolant loses heat and moderates neutrons more effectively, increasing the chances of causing fission, increasing the heat output. When your power requirements decrease, the coolant heats up, does not moderate the neutrons as well and the rate of fission goes down.

An ingenious mechanism but not failsafe as the US Navy has implemented it. One worse case scenario, for example, is a loss of coolant. If necessary, the reactor can be opened to the sea, an infinite heat sink. But by the principles described above, the reaction goes to full power and may progress beyond the point that the flow of sea

water can handle. There is a good description of this in THFRO.

Nevertheless, it would seem such principles, when practical, are preferable to the inherently unstable airframes typified by the F-16 and X-29 fighter planes. As long as people don't put all their faith in them.

Phil Ngai +1 408 982 7840 UUCP: {ucbvax,decwrl,hplabs,allegra}!amdcad!phil

A different RISK? (in-flight control computers)

Peter Ladkin <ladkin@kestrel.arpa.ARPA>
Mon, 6 Apr 87 15:24:58 pst

There is a risk to using flight control computers in military aircraft that I believe hasn't been noted on this list so far. The most relevant instances are in the F-16, F-18 and F-20 aircraft. Two F-20 aircraft have been lost while in airshow routines or practices. The computers are designed to limit control actuations so that the aircraft do not enter accelerated stalls at high G-forces. The control actuations are limited also to approximately 9g positive, since this is currently the limits that a pilot can withstand using current equipment, without losing consciousness. The rate of onset of g forces also contributes to the possibility of losing consciousness. An F-20 is capable of attaining at least a 6.2g per second onset rate.

The risk is that a pilot may plan on losing some brain function to g-forces, without risking that the plane will go out of control in the maneuver. This possibility is entirely due to the presence of the flight control computer. It leads pilots to enter maneuvers in which they do in fact lose consciousness, inadvertently. The F-20 has crashed twice in airshow routines, after the same potential 9g pull-up maneuver, and in the second instance, at Goose Bay, Labrador, the Canadian equivalent of the NTSB found that the pilot's loss of conciousness was directly responsible for the crash.

Were the flight control computer not to assure maneuvering within the envelope in the event of an extreme g maneuver, no pilot would risk loss of control through impaired function, unless in combat.
One, possibly two F-20s and their pilots have been lost through risk-taking while relying on a computer. I understand that pilots have been lost in the F-16 and F-18 in similar situations.

peter ladkin

Fumes from computers and other electronic appliances

Mark W. Eichin <eichin@ATHENA.MIT.EDU>
Mon, 6 Apr 87 14:46:40 EST

According to the advertisments, the version of the HP-41 that is used on the Space Shuttle has a different plastic in the case, which will not outgas under vacuum conditions. Is this a similar problem?

Mark Eichin

VDT related skin cancer?

Chris Koenigsberg <ckk#@andrew.cmu.edu>
Tue, 7 Apr 87 11:47:02 edt

I just had a small round patch of skin cancer removed from my face, under my right eye. I am under 30 years old, and the surgeon said it was highly unusual for someone my age to have such a problem. He said my skin must be highly sensitive, and I would have to be real careful about exposure to the sun in the future, using a blocking sunscreen preparation.

But I am not a heavy tanner or beach-goer. I don't even spend all that much time outdoors. Then the surgeon said, "Oh, you work around computers all day long, don't you?".....and I am now faced with the frightening possibility that my ten years of hacking in close proximity to CRT's is what gave me skin cancer.

I have seen references to studies about the potential danger from CRT radiation but I never paid any attention before. Now I'm inclined to look into the subject - I don't want another skin cancer! The surgeon asked whether it was possible to get a screen with lead shielding on it.

The cancerous growth has been on my face for at least a year, possibly longer. I used VT52's starting in 1977 or 78, Foxes, H19's & VT100's, then primarily a monochrome IBM PC starting in 1981 or 82 for three years. In 1984 I got a Sun 2 workstation, in 1985 I got a pre-release IBM RT. Would the workstations emit more radiation, from their larger screens, than the PC or terminals? Are some brands better shielded than others? Would some different placement angle help lower the dosage hitting my face?

Christopher Koenigsberg, Andrew Systems Administration, Carnegie-Mellon Univ.

Search RISKS using swish-e

THE RISKS DIGEST

Forum on Risks to the Public in Computers and Related Systems

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

Volume 4: Issue 73

Saturday, 11 April 1987

Contents

Unintentional information dissemination

George W. Dinolt <dinolt@Ford-wdl1.ARPA>
Thu, 9 Apr 87 14:05:51 MST

I thought the following article would be of interest to RISKS readers.
The risks of people disposing of equipment who are unfamiliar with the technology used there in can lead to all sorts of interesting problems. GWD

From COMPUTER CURRENTS, Vol 4 #22, 7 April 1987, p68 from the NEWSBYTES UK section by Steve Gold,

BARGAIN COMPUTER HOLDS STATE SECRETS

OXFORD, UK - Irangate had nothing on this one. The "London Times" revealed last month that an Oxford student got more than he bargained for when he bought a second-hand computer for 45 pounds ($68) at WS Surplus Supplies in his home town.

Upon booting the used 64K CP/M computer, Mark Storer found an array of expensive programs available, as well as more than 1,500 files still intact on the machine's 40Mbyte hard disk. When he peeked at the files, Storer realized the computer's origin - The Royal Signals and Radar Establishment in Malvern, Worcestershire.

Aside from being a Ministry of Defense establishment, the Malvern site carries out some very hush-hush research into the kind of things we can't print. Suffice it to say that the files included lists of base personnel, their job descriptions and personal history, and a full inventory, with costs, of the base since 1980!

"They effectively let me walk inside the base and look through their files," said Storer, talking to the press of his find. "NewsBytes UK" understands that the machine has now been returned to the Defense Ministry and that a full investigation is under way.

Computers & Personal Privacy

Steve Thompson <THOMPSON%BROWNVM.BITNET@wiscvm.wisc.edu>
Thu, 09 Apr 87 01:46:43 EDT

From the Friday, 27 March 1987 edition of *The Providence Journal*:

Union official sues Journal for probe into background

PROVIDENCE - The interim administrator of the Providence Newspaper Guild is suing the Providence Journal Co. and Equifax Inc. for $1,050,000, alleging that they illegally used computerized personal information about her as part of an investigation into her background.

In a suit filed Monday [23 March] in U.S. District Court, Susan Zucker, the interim administrator, said that the newspaper employed Equifax to conduct an investigation aimed at providing information on her "character, general reputation, personal characteristics, financial characteristics, mode of living, strengths and weaknesses, estimated net worth, financial difficulties, home surroundings and credit record."

Zucker asserts that Equifax submitted a report containing such information to the Journal company.

She said both companies violated federal law governing how such information may be used, because she was never an employee of the Journal Company nor a candidate for employment, and because she never gave the newspaper nor Equifax permission to review her background.

[Neither of the companies would comment.] ....

I found this notable not only because of the alleged misuse of computerized records, but 1) because of how much information about details of the case was not reported, and 2) that the charged newspaper printed the article at all.

Stephen W. Thompson, User Services Specialist, User Services
Brown U., Box P, Providence, RI 02906 USA (401) 863-3619

Air Traffic Control in the UK

"Lindsay F. Marshall" <lindsay%kelpie.newcastle.ac.uk@Cs.Ucl.AC.UK>
Fri, 10 Apr 87 08:50:55 gmt

A recent report claims that the system installed at West Drayton (which controls Heathrow) fails several times a month. The hardware was installed in 1971 and the only other working version of it (in the UK) is in the Science Museum!! The report says that if the computer were a plane it would have been grounded years ago and that the CAA are not even handed about this situation. (They do admit that the near misses that occur are mostly due to operator error). A spokesman from the CAA has refuted these claims stating that there have been only two failures in 3 months due to software and one failure due to a faulty power supply. He also claimed that the hardware was not obsolete but that it was due for replacement in two years time.

The report was produced from confidential interviews with air traffic controllers by the Institute of Medicine and Avionics (??????)

Sorry if this is a bit vague - it's second-hand information. Lindsay

Air Traffic Control in the USA

Peter G. Neumann <Neumann@CSL.SRI.COM>
Sat 11 Apr 87 14:32:21-PDT

I noted two items recently of interest here.

1. Operational errors by U.S. air traffic controllers increased by 18 percent in the three month period that ended March 26, as compared with the same period a year earlier... Many of the errors appear to be caused by poor cmmunication, lack of coordination and ineffective use of equipment. [From an internal FAA message from Keith Potts, associate administrator for air traffic control, SF Chron, 9 April 1987]

2. Air near-misses were up 29% in 1985 (758) over 1984 and up 42% in 1986 (839) over 1984. [PBS, 9 April 1987] Another source cited 866 near air collisions in 1986, with 497 near-misses on the ground. It also noted that the shortage of controllers had resulted in their being paid overtime three times as much as previously... [SF Chronicle, 10 April 1987]

Re: "Inherently safe nuclear reactors" (RISKS-4.71)

Jim Carter <jimc@CS.UCLA.EDU>
Thu, 9 Apr 87 12:25:08 PDT

In RISKS 4.72 Phil Ngai <{ucbvax,decwrl,hplabs,allegra}!ampcad!phil} writes about reactivity control in American nuclear submarine reactors. In addition to those, all NRC-licensed reactors have the negative temperature coefficient of reactivity he describes. Also, when pressure is lost the boiling in the core greatly reduces reactivity. It also ensures heat removal with the coolant pumps out of action, provided the vessel and pipes are full of water. Kraftwerk Union even has a natural convection reactor without any pumps. These are good examples of inherently safe systems, provided water flood can be assured, as in a bathtub design.

Flooding a naval reactor with seawater would shut it down since the chlorine in the water absorbs neutrons. I believe that river water would not give a sure shutdown unless the pollution level was quite high. In commercial reactors there are large reserves of water loaded with borate, a strong neutron absorber, to be actively injected into the core. Active injection is not inherently safe. A bathtub would be better.

James F. Carter (213) 206-1306
UCLA-SEASnet; 2567 Boelter Hall; 405 Hilgard Ave.; Los Angeles, CA 90024-1600
UUCP:...!{ihnp4,ucbvax,{hao!cepu}}!ucla-cs!jimc ARPA:jimc@CS.UCLA.EDU

Submarine reactor safety

Jim Hunt <c9b-rd%dorothy.Berkeley.EDU@berkeley.edu>
Fri, 10 Apr 87 15:50:24 PST

From RISKS 4.72: (_The Hunt for Red October_, and _Submarines_) ...

The author of "..Red October" has never been underway on a US submarine. He has talked to a lot of people, and taken a civilian tour certainly. He makes a great yarn, and invents some plausable explanations, but (unless someone PUT IN those gross errors I noted) he guessed it all. The reactor coolant is regulated to within a few degrees, and in operation is held much more closely than that, with some variation, soon corrected, upon a change in bell (speed order). It may be that the author knew this, since it is obvious that thermal stress is undesirable, but needed a way to have a core meltdown for plot reasons. (there is also NO installed way to flood the RC, submarines BARELY float as it is) Since this is not in line with comp. risks, the subject should be dropped from this forum. I would like to offer my services as a source of correct information in the future. I won't give away secrets, but it will be the truth. If you, or anyone else has questions on the errors in that book, or US attack submarines in general, feel free to write to me. This is not the first time I have gagged on a statement on submarine operations or equipment as posted in this group.

Jim Hunt hunt@ucbcory.Berkeley.EDU hunt@ucbcory.BITNET (Ex. ET2(SS))

Re: A different RISK? (in-flight control computers) (RISKS-4.72)

Ronald J Wanttaja <ucbcad!ames!uw-beaver!ssc-vax!wanttaja@ucbvax.Berkeley.EDU>
Fri, 10 Apr 87 10:48:39 pst

I don't see this as a risk that can be eliminated without a whole lot of sensing and evaluation of the pilot's real-time condition.

The G-limits programmed in operate on the assumption that the pilot is actively helping keep himself concious... there are physical acts a pilot can take under that will help keep him concious while undergoing Gs. In the Candian F-20 crash, the report mentioned that the pilot had flown the sequence several times that day, and that he was probably somewhat fatigued. It speculated the pilot may have not been as enthusiastic with his anti-G straining, and the G-induced loss of conciousness resulted.

Obviously, the flight computer needs to sense the pilot's physical state, and back off the Gs if the pilot shows signs of going under. Fighter pilots are not going to like this, of course, since it takes an element of control out of their hands. The problem of how to hook up the appropiate sensors to the pilot, while allowing him full freedom of movement and quick, *gentle* disconncection during ejection, is left as a problem for the reader...

Ron Wanttaja (ssc-vax!wanttaja)

Risks"-taking" of in-flight control computers

<eugene@ames-nas.arpa>
09 Apr 87 10:39:10 PST (Thu)

Peter Ladkin writes:
>The risk is that a pilot may plan on losing some brain function to
>g-forces, without risking that the plane will go out of control in the
>maneuver. This possibility ... leads pilots to enter maneuvers in which
>they do in fact lose consciousness, inadvertently.

I think the causality is blurred in this example. I think this is more a case of risk-taking overriding risks (trying). High performance aircraft like the F-16 are actually capable of even greater G turns. We have an aircraft name the HiMAT which I think will take a 20G, but it is a remotely piloted vehicle. When you use words like "due to" and "leads," these are implications against the computer when in fact pilots are pushing their bodies' envelopes and not the plane's envelope. [The computer "made me do it"?]

>Were the flight control computer not to assure maneuvering within the
>envelope in the event of an extreme g maneuver, no pilot would risk
>loss of control through impaired function, unless in combat.

See Top Gun. Try also "simulated combat." I don't vouch for the realism of the movie only the personalities of this type of flyer (push the limits). Remember, the computer is NOT programmed to take the controls from the pilot in event of backout, and it's not clear to me that it

should [Pilot's associate for pilots out there?].

I decided to comment about this note because it was from Peter (a known risk-taker) when some friends and I met him (we went to do the same rock [climb] down in Pinnacles Natl. Mon. [separate parties]). I think the situation is somewhat like putting a computer on own's back which prevents one from climbing above some rating (while trying to push one's skill ever higher).

--eugene miya

Software Risks with Cable TV

<thode@nprdc.arpa>
10 April 1987 0751-PST (Friday)

Cable TV risks attributed to software, and subsequent risks of bodily harm -- From the San Diego Evening Tribune (TV/Radio critic's column), April 9, 1987:

> Pay per view. It's as important to some people as their telephones, and when it doesn't work as well, they get very unhappy.
>
> Like Monday night when the Sugar Ray Leonard - Marvin Hagler middleweight title fight live from Las Vegas went down for the count in thousands of San Diego households. In what Cox Cable general manager Robert McRann calls "a software problem...a programming mixup," 4,510 customers missed part or all of the fight after they paid $30 to $40 for pay-per-view coverage.
>
> People got so upset that Cox had to call the cops when some 300 frustrated people began milling around the lobby at Cox's Euclid Avenue headquarters.

Apparently all ended relatively well. No violence was reported, and Cox customers got refunds and/or vouchers for future cable pay-per-view events. Cox spokespeople asserted that this was their first serious problem in over two years of pay-per-view baseball games, movies, and other special events such as the recent Wrestlemania, for which over 10,000 people (!) signed up.

--Walt Thode (thode@NPRDC)

My Broadcast [The UNIX rwall problem]

Jordan K. Hubbard <jkh@violet.Berkeley.EDU>
Thu, 2 Apr 87 10:45:46 PST

> [The following message was submitted to RISKS by 6 different people. I initially thought it might already have been widely circulated, but its repeated receipt has led me to include it here anyway. PGN]

By now, many of you have heard of (or seen) the broadcast message I sent to

the net two days ago. I have since received 743 messages and have replied to every one (either with a form letter, or more personally when questions were asked). The intention behind this effort was to show that I wasn't interested in doing what I did maliciously or in hiding out afterwards and avoiding the repercussions. One of the people who received my message was Dennis Perry, the Inspector General of the ARPAnet (in the Pentagon), and he wasn't exactly pleased. (I hear his Interleaf windows got scribbled on)

So now everyone is asking: "Who is this Jordan Hubbard, and why is he on my screen??"

I will attempt to explain.

I head a small group here at Berkeley called the "Distributed Unix Group". What that essentially means is that I come up with Unix distribution software for workstations on campus. Part of this job entails seeing where some of the novice administrators we're creating will hang themselves, and hopefully prevent them from doing so. Yesterday, I finally got around to looking at the "broadcast" group in /etc/netgroup which was set to "(,,)". It was obvious that this was set up for rwall to use, so I read the documentation on "netgroup" and "rwall". A section of the netgroup man[ual] page said:

> ...
>
> Any of three fields can be empty, in which case it signifies a wild card. Thus
>
> universal (,,)
>
> defines a group to which everyone belongs. Field names that ...
> ...

Now "everyone" here is pretty ambiguous. Reading a bit further down, one sees discussion on yellow-pages domains and might be led to believe that "everyone" was everyone in your domain. I know that rwall uses point-to-point RPC connections, so I didn't feel that this was what they meant, just that it seemed to be the implication.

Reading the rwall man page turned up nothing about "broadcasts". It doesn't even specify the communications method used. One might infer that rwall did indeed use actual broadcast packets.

Failing to find anything that might suggest that rwall would do anything nasty beyond the bounds of the current domain (or at least up to the IMP), I tried it. I knew that rwall takes awhile to do its stuff, so I left it running and went back to my office. I assumed that anyone who got my message would let me know.. Boy, was I right about that!
After the first few mail messages arrived from Purdue and Utexas, I begin to understand what was really going on and killed the rwall. I mean, how often do you expect to run something on your machine and have people from Wisconsin start getting the results of it on their screens?

All of this has raised some interesting points and problems.

1. Rwall will walk through your entire hosts file and blare at anyone and everyone if you use the (,,) wildcard group. Whether this is a bug or a feature, I don't know.

2. Since rwall is an RPC service, and RPC doesn't seem to give a damn who you are as long as you're root (which is trivial to be, on a work-station), I have to wonder what other RPC services are open holes. We've managed to do some interesting, unauthorized, things with the YP service here at Berkeley, I wonder what the implications of this are.

3. Having a group called "broadcast" in your netgroup file (which is how it comes from sun) is just begging for some novice admin (or operator with root) to use it in the mistaken belief that he/she is getting to all the users. I am really surprised (as are many others) that this has taken this long to happen.

4. Killing rwall is not going to solve the problem. Any fool can write rwall, and just about any fool can get root priviledge on a Sun workstation. It seems that the place to fix the problem is on the receiving ends. The only other alternative would be to tighten up all the IMP gateways to forward packets only from "trusted" hosts. I don't like that at all, from a standpoint of reduced convenience and productivity. Also, since many places are adding hosts at a phenominal rate (ourselves especially), it would be hard to keep such a database up to date. Many perfectly well-behaved people would suffer for the potential sins of a few.

I certainly don't intend to do this again, but I'm very curious as to what will happen as a result. A lot of people got wall'd, and I would think that they would be annoyed that their machine would let someone from the opposite side of the continent do such a thing!

Jordan Hubbard, jkh@violet.berkeley.edu, (ucbvax!jkh)
Computer Facilities & Communications, U.C. Berkeley

Search RISKS using swish-e

THE RISKS DIGEST

Forum on Risks to the Public in Computers and Related Systems

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

Volume 4: Issue 74

Tuesday, 14 April 1987

Contents

Re: A different RISK? (in-flight control computers)

<utzoo!henry@ai.toronto.edu>
Mon, 13 Apr 87 20:18:20 EDT

> The risk is that a pilot may plan on losing some brain function to
> g-forces, without risking that the plane will go out of control in the
> maneuver. This possibility is entirely due to the presence of the
> flight control computer...

Not very plausible at the current state of the art. The flight control computers are *not* capable of preventing the aircraft from going out of control; they merely prevent one or two specific types of failure (e.g. breaking the aircraft) that are so clearly undesirable that they can be

unquestionably ruled out.

In fact, because the problem has gotten a lot more visible of late, serious consideration is now being given to *awarding* the flight-control computers such powers, to save the aircraft and the pilot! The tentative intent is to sense unconsciousness in some manner, signal the pilot that the computer thinks he is unconscious, and if this brings no response, to take over and restore (at least) level flight. Nobody, repeat nobody, is suggesting that the computer try to continue the maneuver the pilot was attempting.

> ...The F-20 has crashed twice in airshow routines, after the same potential
> 9g pull-up maneuver...

Several other crashes, such as that of the British Aerospace attack-configured Hawk prototype, have been tentatively attributed to G-LOC (G-induced Loss Of Consciousness). And there is considerable suspicion that it may account for other unexplained crashes of very-high-performance fighters in recent years.

What is new about the recent fighters is that they can get into high-G situations much more suddenly than older planes could. In older fighters, loss of blood flow to the brain was gradual, and symptoms like tunnel vision could be relied on as warnings. The new fighters can pile on the Gs so quickly that blood flow cuts off almost instantaneously, leaving the brain running on stored oxygen for a moment and then suddenly losing consciousness when that runs out.

> Were the flight control computer not to assure maneuvering within the
> envelope in the event of an extreme g maneuver, no pilot would risk
> loss of control through impaired function, unless in combat.

"Within the envelope" does not equal "under control", as the F-20 pilots assuredly knew. I find it extremely implausible that they deliberately risked loss of control by relying on the computers; the computers (well, actually, the programs) aren't that good and the consequences of going out of control can be too final.

Henry Spencer @ U of Toronto Zoology {allegra,ihnp4,decvax,pyramid}!utzoo!henry

---

Trojan Horse alert

<forags%violet.Berkeley.EDU@berkeley.edu>
Tue, 14 Apr 87 11:41:50 PDT

Yet another Trojan horse is loose, alas. Several related messages have circulated on comp.sys.ibm.pc about this one.

- Al Stangenberger, Forestry, U.C. Berkeley

> From: w8sdz@brl-smoke.ARPA (Keith B. Petersen)
> Newsgroups: comp.sys.ibm.pc
> Subject: Re: Numerous requests for ARC.EXE
> Date: 9 Apr 87 02:46:14 GMT

> Organization: Ballistic Research Lab (BRL), APG, MD.

> ARC513 is a trojan horse. The latest version of SEA's ARC is ARC520
> and it's available from SIMTEL20 as PD:<MSDOS.ARC-LBR>ARC520.COM.

The Limits of Software Reliability

Brian Randell <brian%kelpie.newcastle.ac.uk@Cs.Ucl.AC.UK>
Tue, 14 Apr 87 08:46:01 gmt

The "Subject:" field is the title of a paper, by R.L. Enfield, in Technology Review 90,3 (April 1987), pp.36-43. The paper is worthwhile as a readable account, for a general audience. (The author is stated to have a led a study of the fault tolerance of the programs used in the Aegis ship combat system.)

Re: Conrail Sale Funds Transfer -- and a 747 overflow

<utzoo!henry@ai.toronto.edu>
Mon, 13 Apr 87 20:18:13 EDT

> The sale of Consolidated Rail Corp. almost blew some fuses at the
> Treasury Dept. Because Treasury's computers can only handle single
> transactions of up to $1 billion...

This is reminiscent of the famous, possibly apocryphal, disaster that hit the airline reservation systems when the first 747s entered service. It was the first airliner that could carry more than 255 passengers...

Henry Spencer @ U of Toronto Zoology

Re: VDT related skin cancer?

<utzoo!henry@ai.toronto.edu>
Mon, 13 Apr 87 20:31:31 EDT

To keep some perspective on this, note that there is no unusual incidence of skin cancer among TV program directors, who also spend their lives staring at monitors at close range -- often older, less-well-shielded monitors.

> The surgeon asked whether it was possible to get a screen with lead shielding

Add-on shields exist, I believe. It is not clear that they are worthwhile. Modern monitors have to meet quite severe X-ray emission limits. Consider having the X-ray output of your display measured first. Somebody at CMU ought to be equipped to do this.

> Would the workstations emit more radiation, from their larger screens,
> than the PC or terminals?

There isn't *necessarily* any correlation with screen size. X-ray energy is related to beam accelerating voltage; intensity is proportional to beam current. A bigger screen will need higher current to get the same brightness over a larger area, but will also spread the emissions out more. At first glance I suspect that size won't make much difference overall. Voltage is chosen by several criteria, but I don't think size has a lot to do with it. I am not an expert on CRT design, mind you.

> Are some brands better shielded than others?

Different brands using the same monitor will be similar, and it's not always easy to find out who Sun (for example) buys monitors from. I would expect to see little variation in any case.

> Would some different placement angle help lower the dosage hitting my face?

Probably not. Distance will make a difference, as will shielding (even a sheet of glass -- soft X-rays are not very penetrating).

Don't overlook other possible causes: chemical emissions, acceleration of dust particles by static electricity, or sheer chance. Granted that the doctor said it was unusual; many unusual things happen every day.

Henry Spencer @ U of Toronto Zoology

Re: Open University Fire

<utzoo!henry@ai.toronto.edu>
Mon, 13 Apr 87 20:18:03 EDT

> ... eventually [the loss of work] seems to have come down to a couple of
> months as most people had personal back-ups of critical data!!

It should be noted that this isn't invariably true. When U of T had a major fire ten years ago, far too many things -- including some valuable software products -- existed only in one building, the one that had the fire. We were lucky: most of the computer facilities received only minor water and smoke damage. (In fact, the Unix system stayed up through it all, going down only when the power to the whole building was cut, after the fire was largely under control!)

An awful lot of people suddenly became much more conscientious about offsite backups (and fire safety in general) after that. I do wonder how long the effect lasted, though. The building has been rebuilt, and now has many more computers in it. How many of them have complete offsite backups?

Henry Spencer @ U of Toronto Zoology

DES Second Review Notice [on the RISKS OF STANDARDS?]

David M. Balenson <balenson@icst-ssi.ARPA>
Fri, 10 Apr 87 14:46:53 EST

[Please contact David if you want a copy of the notice. The notice itself did not seem suitable for RISKS, but the risks associated with encryption standards was sufficiently relevant to post this message. PGN]

For your information, there is a copy of the Federal Register Notice regarding the second review of Federal Information Processing Standard (FIPS) 46, Data Encryption Standard (DES). Written comments are solicited by June 4, 1987. The more comments we receive, the better NBS will be able to take a stance regarding the future of DES.

David M. Balenson (DB) [balenson@icst-ssi.ARPA]
Security Technology Group / Computer Security Division
National Bureau of Standards, Technology A216, Gaithersburg, Maryland 20899
(301) 975-2910

Bank Computers (Not ATM's)

Ken Ross <munnari!mulga.oz!kar@seismo.CSS.GOV>
Sun, 12 Apr 87 14:00:39 +1000

A little while ago, I went to the bank to withdraw $1200 to buy a saxophone. I filled in a withdrawal form and presented it to the teller. He punched the data into his terminal, debiting my account $1200. He then asked what denomination notes I would like. "Unfortunately," he said, "we're out of 50's and 100's." (Here in Australia, we have notes with the following denominations: $100, 50, 20, 10, 5 and 2. Smaller denominations are in coins.)

I did not want to carry sixty $20 notes around with me, and I didn't want a bank cheque either. I asked him to "undo" the transaction, and said I'd come back later. The teller assured me that the only way that it could be done would be to redeposit the $1200 into the same account. So, that is what happened.

In the state of Victoria (where the story takes place) there is a state tax of 3 cents in every hundred dollars on deposits. Thus the net effect of the whole affair was that I paid 36 cents tax.

I didn't bother pursuing the matter; a postage stamp costs 36 cents. However, there is a potential risk here in the definition of when a transaction has occurred. I am not a lawyer, but I suspect that legally a transaction is not complete until both parties involved are "satisfied". Hence the withdrawal of the money was not complete at the stage when the teller informed me of the unavailability of high-denomination notes. As I could reasonably expect to get high-denomination notes, I should have been able to abort the transaction at this stage.

But, because it had been entered on the computer, the transaction had been completed as far as the bank was concerned.

If the computer software had been better designed then there should have been a mechanism to abort the transaction right up until the customer leaves. I do not think that a feature like this would cause any further problems, although I am not familiar with bank procedure.

UUCP: {seismo,mcvax,ukc,ubc-vision}!mulga!kar CSNET: kar%mulga.oz@australia

[Even though the case is small peanuts (or eucalyptus pods?), it illustrates a general problem: the need for a complete transaction UNDO that leaves NO adverse side-effects. It is not really so much a case of an improper atomic action. On the other hand, the bank might take the attitude that TWO transactions were required, and therefore it needed to charge for BOTH! PGN]

The Marconi Affair [Follow-up on RISKS-4.72]

Brian Randell <brian%kelpie.newcastle.ac.uk@Cs.Ucl.AC.UK>
Tue, 14 Apr 87 09:55:13 gmt

The essence of the latest Computer News story is that a mysterious Ministry of Defence department has begun an investigation into the affair. ``The MoD is adamant that the investigation involves its own "Serious Crimes Squad". It also suggests the enquiries involve alleged fraud on defence contracts. Yet MPs, and even MoD press officers were at first unaware of the existence of the squad. A Ministry of Defence spokesman said: there is nothing sinister. The Serious Crimes Squad of the Ministry of Defence was first mentioned in the Police Almanac 10 years ago. But library files do not show that the squad has been involved in any previous allegations of fraud in defence contracts.'' (The story goes on to mention that the investigation is based at Portsmouth, where Sharif, who was found hanged, is known to have worked for Marconi Underwater Systems.)

Search RISKS using swish-e

THE RISKS DIGEST

Forum on Risks to the Public in Computers and Related Systems

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

Volume 4: Issue 75

Monday, 20 April 1987

Contents

Flight control risks

Peter Ladkin <ladkin@kestrel.ARPA>
Wed, 15 Apr 87 14:54:23 pst

Henry Spencer notes that the flight control on an F16 (etc) does not prevent the pilot from losing control of the aircraft. He is correct to the letter. To my knowledge, there is no aircraft yet built which is guaranteed to be stall-free, spin-free and tumble-free.

Let me be more precise, and unfortunately more lengthy. I was trying to convey the idea that because of fly-by-wire design decisions, there are different risks to flying a new-generation fighter.

An aircraft may enter an accelerated stall at high speed in a sharp turn. An

F16 airframe is certainly capable of this, but is control limited since the pilot probably isn't. The pilot believes he or she may thus roll and haul back, strain and black-out, and not have to cope with an accelerated stall while having no vision. With real control actuators in the F16, a pilot would have to be much more sensitive on the stick, and probably couldn't plan to tolerate routine black-outs. The risks have changed - pilots now sometimes lose consciousness, and have little or no motor control for up to a minute when they regain it. That's a dive into the ground from 60,000 feet.

This is rather like the ATM example. Usually the transaction is finished when you remove your card, but not always, it seems. With a real teller it would be. But a real teller might make a transcription mistake. The risks have changed.

The Airbus example is relevant here, also. Using computer direction to maintain maximal angle of attack on a go-around might lead to disaster if in a microburst rotor, since the winds change faster than the aircraft can respond (as in the DFW accident). I'm sure the airbus people would have thought of that - except that we don't yet know what exactly happens in a microburst, so how can we be assured of the control logic? The computer controls the aircraft better than a human can follow a flight director, but a human can improvise, sometimes, in these unknown situations. The risks have changed - but maybe I'm preaching to the converted?

peter ladkin

``More on risky high-g piloting''

Tom Perrine <Perrine@LOGICON.ARPA>
16 Apr 87 16:47 PDT

From the "Safety" column in the March 30 Aviation Week and Space Technology, the magazine-provided abstract follows:

Northrup Corp.'s F-20A Tigershark prototype fighter aircraft was flying an authorized practice demonstration at the Goose Bay Airport, Labrador, Newfoundland, on May 14, 1985, in preparation for performances at the upcoming Paris air show. During the final aerobatic maneuver of the 5-min. flight, the aircraft deviated from the planned profile and entered a shallow wings-level descent. The descent continued until the aircraft struck the ground, killing the pilot, David Barnes.

The Canadian Aviation Safety Board determined that the Northrup pilot became incapacitated during or following the final high-g pull-up maneuver and did not recover sufficiently to prevent the aircraft from striking the ground. Initial portions ran in Aviation Week and Space Technology Mar 23, p. 75; Mar 16, p. 89.

[[[End of Abstract]]]

This 3rd part of the series presents the conclusions of the CASB. This is related to Risks only in that previous contributions have suggested that pilots were beginning to depend on the computer to save them in GLC (G-induced Loss of Conciousness) situations and the CASB findings *do not*

support this hypothesis. In fact, this civilian pilot "had not received formal aeromedical training pertaining to the GLC phenomenon and no evidence was found that GLC training was required prior to participation in high-g demonstration flights."

There were also pilot medical conditions and other contributing factors. It would seem that this was a training and human risk, rather than a computer-related risk.

Tom Perrine

Checklist stops risks?

<Beckman@DOCKMASTER.ARPA>
Fri, 17 Apr 87 08:06 EDT

1. A couple of weeks ago, my VCR started "malfunctioning." It would turn the TV screen to noise whenever I pushed the TV/VCR button to TV (it does not record without the "TV" being "on"), and so would not record. It also did not play back. I got a picture (very muddy) and not much sound. Since my son (age 2.5) had been "playing" with it the day before, I tried to find out what he had done (if anything). I checked the connections, a few buttons in the "control panel" in front, the channel on the front (with cable, you just leave it on channel 3), but could find nothing wrong. I did not look in the manual for instructions on initial startup. The problem? The channel select IN BACK, a small switch which selects either channel 3 or 4 had been switched to 4.

Last week, my radio in the car starting "malfunctioning" (the normal stations were not coming in, etc). I still had not learned the VCR lesson, and it took me several days to find out he (my son again) had hit the FM/AM button.

If I had a simple checklist, I would have easily and quickly solved both of these "problems." Now I am wondering about more complicated systems (airplanes, power plants, etc.). What kind of things are on their "checklists"? The simple variety (check fuel gauge), or more elaborate items?

Joseph

[You forgot that your offspring is very resilient. PGN]

Radiation risk at airports?

Paul Stewart <beach!paul@rand-unix.ARPA>
Mon, 20-Apr-87 00:40:59 PDT

On Saturday, April 18, the major wire and news services carried a story, attributed to the New York Times, saying that the FAA was about to start testing of a prototype neutron beam-based system for detecting the nitrogen in explosives that might be in luggage/cargo loaded into plane cargo holds. This is a computer-based system that bombards luggage or other cargo with a "beam of slowed neutrons" and uses a computer system to analyze the signature of the resulting gamma radiation emissions to characterize for the

potential presence of explosives.

The Associated Press inaccurately suggested that the manufacturer of this equipment was a firm named "Thermedics." The actual NYT article gives much more detail and accurately names the manufacturer as "Science Applications International Corp." of Sunnyvale.

Some months ago, when this technology was originally mentioned in the press, there was some discussion of the radiation problems inherent with this sort of technology. While one would assume care would be used to make sure animals traveling as cargo are not subjected to a neutron beam, the problem of secondary radiation effects on the clothes, foods, medications, and everything else that travels as cargo/luggage seems to be glossed over by the press. While normal X-ray technologies do not produce secondary radiation at conventional power levels, neutrons are extremely energetic and in fact this explosive detection system appears to be depending on secondary radiation for its very operation!

When this system was first discussed in the press some months ago, there was mention of the problems of cargo and luggage becoming "slightly radioactive" as a result of being subjected to the "slowed neutron beam." The current discussion in the press seems to be avoiding this issue entirely, instead mentioning that the people operating the equipment will not be subjected to more than "government standards" for radiation exposure (many persons seem to feel that these standards allow far too much exposure as it is).

The question then, for anyone who understands this technology or knows about Science Applications International, is: what will happen to luggage, cargo, etc., possibly including foods and other items that can be ingested or will be in close proximity to persons for long periods of time, after passing through such neutron beam systems once or possibly many times in the course of complex or multiple trips? Are airline passengers to be subjected to the radioactive luggage and cargo simply because the emission levels meet "government standards"? Will the frequent traveler be at greater risk than the occasional traveler? What is the real story about these systems?

In case you're wondering who will be the first guinea pigs for this technology, it's the folks in the SF Bay area. San Francisco International (SFO) is slated to get the first prototypes of these devices sometime quite soon for at least a 4-week trial. The equipment is then to be tested at other major airports and the FAA hopes to have it in widespread use within 2 years. Apparently the prototypes to be tested are "improved" versions of an earlier model that required 30 seconds per test--the new equipment bombards the target material for 6 seconds (possibly longer if the typical conveyer and luggage problems cause clogs on the transport system). Of the two prototypes, one supposedly uses a continuous neutron emitter based on an internal chunk of some radioactive material, while the other uses a "turn-offable" system for generating the neutrons.

Can anyone out there shed some light on the risks associated with this technology?

[The computers in this system may or may not present risks,

e.g., if the computers are involved in control, or if the signature analysis is faulty. In any case, the risk issues are interesting enough to warrant some KNOWLEDGEABLE discussion here. Let's avoid SPECULATIONS, PLEASE. PGN]

How to post a fake

Chuq Von Rospach <sun!plaid!chuq@seismo.CSS.GOV>
Sat, 18 Apr 87 10:10:56 PDT

To: darrell@beowulf.ucsd.edu, mod-back

> I'm curious: how can you fake a posting without being root? When I post anything to mod.os (er, excuse me, comp.os.research) I'm always listed as the sender. Not wanting to be the bad guy I've never tried to crack it, but I am curious as to the hole that causes the problem.

Darrell asks an interesting question, and I might as well let everyone know while I'm at it.

As background, be aware that USENET has a major security hole, in that there is no way for the program rnews to know where a message came from. It has to implicitly trust the information in the header of the message. While uucp does site verification across the net, that information is not passed along through uux to the executed program on the other side. It has to trust the data it gets.

This leads to a trivial hack for creating bogus and untraceable messages. Take an existing message (I borrowed this one from mod.announce):

```
Path: sun!cbosgd!mark
From: mark@cbosgd.ATT.COM (Mark Horton)
Newsgroups: mod.announce,news.announce.important
Subject: mod.announce is being renamed news.announce.important
Message-ID: <3525@cbosgd.ATT.COM>
Date: 13 Apr 87 15:09:20 GMT
Organization: AT&T Bell Laboratories, Columbus, Oh
Lines: 9
Approved: mark@cbosgd.MIS.OH.ATT.COM
Xref: sun mod.announce:24 news.announce.important:1
```

This is your template. Now, change the header lines to fit, and delete the Xref line:

```
Path: cbosdg!mark
From: mark@cbosdg.ATT.COM (Mark Horton)
Newsgroups: mod.announce
Subject: Newgroup renaming is a failure, film at 11.
Message-ID: <3.14159@cbosdg.ATT.COM>
Date: 1 Apr 87 00:00:00 GMT
Organization: The Backbone Cabal, Inc.
Lines: 9
```

Approved: mark@cbosdg.MIS.OH.ATT.COM

Don't worry about the # of lines, inews will be nice enough to adjust it for you. Store that in a file, add the message body to it, and execute:

% /bin/rnews < file

rnews will read it just as if it had come over the network, and install it. It believes everything you said in the header. When it passes it along, the Path: becomes "sun!cbsogd!mark" and it gets passes along just like a real message. The only place where this is traceable is the Path variable, because you can see that my site is at the beginning of the list of real paths. You can avoid this in a couple of ways if you want to be real sneaky:

o the kremvax syndrome: instead of having a single address in the path, put in a bunch:

Path: kremvax!nsacyber!prarie!wobegon!himom!cbosdg!mark

depending on your ingenuity, you make make it almost impossible to tell where the message joined the net for real.

o drop out of the loop: even more fun, rather than execute rnews on YOUR site, execute it on someone else's.

% uux - -z ihnp4\!rnews < file

the Path is now "ihnp4!cbosdg!mark" and your own site is nowhere to be seen. Completely untraceable, unless someone wants to compare uucp's LOGFILE entry times with news 'log' entries and backtrack. Which assumes that they figure out it is happening before they flush the logs. And that they have the time, and care.

That's how you forge messages. And as long as the uucp links exist, there is no way to fix this, because a vital piece of information isn't passed out of uucp.

The possibilities are endless, of course. You can not only post April Fool's messages, but post messages FOR people that they can never prove they didn't post. completely untraceable. You can change your name, your machine, your religious background, all untraceable. Possibly even skip out on child support, if you find the right control message.

Kids, don't try this at home! These people are paid professionals, and know the risks involved... (grin)

chuq (next week, how to kick a site off the net with cancel messages!)

[For those of you who never saw the KREMVAX 1984 April Fools' Day hoax, see ACM SIGSOFT Software Engineering Notes. July 1984. vol 9 no 4. PGN]

---

faking news postings

Rob Robertson <philabs!rob@briar>
Mon, 20 Apr 87 14:40:47 EST

The only place you can be traced using chuq's "posting techniques" is the log files. In the `uux - -z ihnp4!rnews < file` example, the machine and user name will appear in ihnp4's LOGFILE or HDB's uucico, and uuxqt logs.

I'm not sure but have a funny feeling one can trace the user (by logs) if he posts it on his machine, beside having his machine on the path list.

The brahms people did a good job of tracking down a person faking articles by using log files.

rob

Re: Bank Computers (Not ATMs)

Kuhn <kuhn@ICST-SE>
Wed, 15 Apr 87 15:29:23 est

> I did not want to carry sixty $20 notes around with me, and I didn't want a
> bank cheque either. I asked him to "undo" the transaction, and said I'd come
> back later. The teller assured me that the only way that it could be done
> would be to redeposit the $1200 into the same account...

This may be a people problem rather than a software design problem.

I spent the first three years of my career writing communications interfaces for ATMs for one of the major computer vendors. In the process, I became familiar with the computing systems of several Washington, D.C. banks. For each transaction type, there is a "correction" transaction code that will reverse the effects of its corresponding "normal" tran code. This follows manual accounting procedure that requires errors to be explicitly backed out by a separate entry rather than simply erased. At least two of the banks that I did work for monitored their tellers to keep track of who made errors, when, what kind of error, etc. If Ken Ross's bank has a system like this, and the tellers are aware of it, they might prefer not to use a correction transaction that will show up on a report to their supervisor.

Correction to Conrail Sale Funds Transfer (RISKS 4.72)

Mark Brader <msb@sq.com>
Tue, 14 Apr 87 10:02:59 EST

> [I'm surprised that someone was smart enough to know about the $1
> billion problem before it really did "blow a fuse". Who knows where
> the $600,000 million might have ended up!... (Chuck Weinstock)]

!!!!

Risks of thinking of UK billions in a US story? This is the second error of this off-by-000 type to make it to the net in a week or two (the last one was in sci.astro)...

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

[Fortunately Chuck's extra zeroes were detectable from context... PGN]

"Reliability Theory Applied to Software Testing" in HP Journal

Rich Rosenbaum <rosenbaum%boehm.DEC@decwrl.DEC.COM>
Wednesday, 15 Apr 1987 10:18:21-PDT

The April 1987 issue of the Hewlett-Packard Journal contains a short (four page) article entitled "Reliability Theory Applied to Software Testing."

From the abstract:

> The execution-time theory of software reliability is extended to the software testing process by introduction of an accelerating factor. It is shown that the accelerating factor can be determined from repair data and used to make prerelease estimates of software reliability for similar products.

The article describes how the model was applied to the firmware for two HP terminals.

(Subscriptions to the HP Journal are available without charge from Hewlett-Packard Journal, 3200 Hillview Avenue, Palo Alto, CA 94304).

Search RISKS using swish-e

Report problems with the web pages to the maintainer

Search RISKS using swish-e

THE RISKS DIGEST

Forum on Risks to the Public in Computers and Related Systems

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

Volume 4: Issue 76

Wednesday, 22 April 1987

Contents

Risks of Warranties

Jim Horning <horning@src.DEC.COM>
Tue, 21 Apr 87 15:04:03 PDT

ABACUS, vol. 4, no. 3, Spring 1987 contains the results of ABACUS Competition #3, which invited readers to submit actual examples or parodies of software disclaimers of warranty.

The winner is included as a format example in the user manual of the Horstmann Software Design product, ChiWriter:

> Cosmotronic Software Unlimited Inc. does not warrant that the functions contained in the program will meet your requirements or that the operation of the program will be uninterrupted or error-free.
>
> However, Cosmotronic Software Unlimited Inc. warrants the diskette(s) on which the program is furnished to be of black color and square shape under normal use for a period of nineyt (90) days from the date of purchase.
>
> NOTE: IN NO EVENT WILL COSMOTRONIC SOFTWARE UNLIMITED OR ITS

> DISTRIBUTORS AND THEIR DEALERS BE LIABLE TO YOU FOR ANY DAMAGES,
> INCLUDING ANY LOST PROFIT, LOST SAVINGS, LOST PATIENCE OR OTHER
> INCIDENTAL OR CONSEQUENTIAL DAMAGES.

The runner-up is from the Haven Tree Software Limited program Interactive EasyFlow:

> We don't claim Interactive EasyFlow is good for anything--if you think
> it is, great, but it's up to you to decide. If Interactive EasyFlow
> doesn't work: tough. If you lose a million because Interactive EasyFlow
> messes up, it's you that's out the million, 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 really want to include any disclaimer at all, but our lawyers
> insisted. We tried to ignore them but they threatened us with the attack
> shark at which point we relented.

These remind me of the software order form I received some years ago requiring me to sign a statement acknowledging that the only warranty made by DJ AI Systems was that they owned the copyright on the software being ordered.

Jim H.

Re: Checklist stops risks?

Jerome H. Saltzer <Saltzer@ATHENA.MIT.EDU>
Wed, 22 Apr 87 12:32:30 EST

Joseph Beckman suggests that his VCR and auto radio problems might be reduced by checklists. Probably so. There is a more subtle technology RISK hiding here, one that I notice almost every time I find that a computer has appeared in the control path for an auto radio, a VCR, an automatic washer, or a toaster oven: the device acquires a whole host of new features, options, and state memory that it didn't use to have. As a result you can't run it without a checklist.

Lots of things don't need a checklist. My old toaster certainly didn't need one. But judging from the frequency of mistakes, my new one seems to. A real RISK arises when someone hi-tech's a traditional design, pushing its functional spec over the threshold at which the average user needs a checklist to run it, and then sells this improvement to an unsuspecting and unprepared user community.

Jerry Saltzer

> [Jerry, Many thanks. This raises the desire for CONSISTENCY of code with
> specifications where the system must do NO MORE AND NO LESS than
> specified. Of course, it is likely to do all sorts of things that are
> not specified, and therein lie all sorts of risks. Trying to specify the

action required for EVERY STATE in the state space is an important but very difficult task. (How many of you have fallen on the EMACS bug that results in your being totally HUNG, where even ^G does not work? <Don't answer.>) PGN]

Newer highly maneuverable planes on board and checklists

Eugene Miya <eugene@ames-nas.arpa>
Tue, 21 Apr 87 10:04:09 PDT

Two added notes to existing topics.

There is a recent Aviation Week which mentions a program to make even more maneuverable planes (but not higher G), but I still wonder if it's not more a matter of screening pilots to withstand force. Not unlike recent DARPA comments that maybe 1 in 3 programmers can program new parallel architectures.

Regarding checklists: we have some automated checklist work here. Originally they thought they wanted to put more control into the checklist but decided to separate the control from the check (safer). We should make things easier to use up to a point.

I refrain from comment on slow neutrons. I would worry more about film than food (but that's not my area). SAIC is a scientific body shop with offices all around the country. I was approached by them to work as a contractor at a spook Agency.

--eugene miya, NASA Ames

Aircraft risks

Peter Ladkin <ladkin@kestrel.ARPA>
Tue, 21 Apr 87 13:57:54 pst

Tom Perrine thinks I am suggesting that pilots are willing to risk GLC episodes in the new planes. I am not suggesting this.

I am suggesting that they are more willing to risk a black-out, since the danger of accelerated stalls is moderated. Consequently they risk GLC episodes when they are tired, hard-worked, or simply (according to the air force) away from it over the weekend. A computer is in the loop. My argument is that it makes the scenario more likely.

One possible source of confusion - a blackout is not a loss of consciousness. Blackouts are loss of vision, caused by the collapse of the retinal arteries, and are easily reversed by unloading the Gs.

peter ladkin

Neutron beam detection [RISKS 4.75]

Scott Dorsey <kludge%gitpyr%gatech.gatech.edu@RELAY.CS.NET>
Tue, 21 Apr 87 11:50:35 edt

I can't imagine anything worse that one could do to luggage than bombard it with slow neutrons. The last time I flew commercial, I was carrying about $200 worth of motion picture film in my luggage, and I would be very upset if it had been fogged. Lots of vacationers carrying their vacation pictures will be very upset. Next time I'm taking the lead sheathing...

In addition, what happens to digital electronics when they are hit with slow neutrons? I assume the levels of radiation are low enough not to permanently damage watches, calculators, etc., but it may well be enough to change the state of logic. Logic, like the digital timer used to set off the explosive device that was hidden in the luggage, which goes off in the airport.

A machine which detects nitrogen chains may also detect things like ammonia if it cannot discriminate between long and short chains. Some explosives (like ammonium nitrate) are reasonably safe when not in the presence of an activator, and have reasonable industrial uses. Pity the fertilizer salesman whose sample case is confiscated.

Worst of all, this could lead to a false sense of security; there are lots of nitrogenless explosives out there. Two-part explosives aren't all that hard to come by.

I don't like the idea of pumping hard radiation into luggage. It's just a bad idea in general. Might be good for disinfecting your clothes, though.

Scott Dorsey Kaptain_Kludge
ICS Programming Lab (Where old terminals go to die), Rich 110,
Georgia Institute of Technology, Box 36681, Atlanta, Georgia 30332
...!{akgua,allegra,amd,hplabs,ihnp4,seismo,ut-ngp}!gatech!gitpyr!kludge

Search RISKS using swish-e

THE RISKS DIGEST

Forum on Risks to the Public in Computers and Related Systems

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

Volume 4: Issue 77

Thursday, 23 April 1987

Contents

'Hackers' hit the Jackpot

Michael Bednarek <munnari!murdu.oz!u3369429@seismo.CSS.GOV>
Thu, 23 Apr 87 17:27:22 EST

Paraphrasing a well-known motto:
The Benefits to Individuals in Computer Systems

'Hackers' hit the Jackpot, by John England
The Sun, Melbourne, 23-Apr-1987

BONN, Wed. - Computer experts have cracked the codes of West Germany's most popular poker machine.
They are selling computer print-outs giving the machine's play programs for $6500 and people are embarking on money-spinning raids on pubs and amusement arcades.
Even better, if a person is caught using the system there is nothing to fear. West Germany does not have a law saying it is illegal to fool a machine.

The ruse came to light when three students made a "hit" on a Cologne pub which has four machines.

Police were called after the students won the jackpot on each of the machines within minutes and a search revealed a computer print-out giving the machines' play programs.

Police believe the students, from Brunswick University where a technical department checks poker machines to make sure they comply with the payout law, were the "hackers" who cracked the code.

The makers are hurrying to change their programs but, as a spokesman admitted: "You can't fix 160,000 machines overnight - or stop the hackers cracking the new code!"

Fidelity Mutual Funds Money Line feature

Barry Shein <bzs@bu-cs.bu.edu>
Thu, 23 Apr 87 01:50:10 EDT

From: chris@leadsv.UUCP (Chris Salander)
Newsgroups: misc.invest
Date: 22 Apr 87 19:54:17 GMT
Organization: LMSC-LEADS, Sunnyvale, Ca.
Summary: BEWARE!!! Computers gone mad!

Fidelity Investments has a feature on their Mutual Funds called the Money Line. Every quarter or every month their computers will call the computers at your bank and withdraw a specified amount of money from your checking or savings account and invest it into a particular fund.

I have been severely victimized by this feature and have lost control of my checking account because of it. As a warning to the rest of you here is my story:

January 1986
I sign up for 3 of Fidelity's funds and invest some $. I ask for the Money Line feature (once every quarter) on each account and give them my electronic banking number and checking account number.

May 1986
Investments doing well. Money Line feature on each fund was never activated. I invest in one more fund, Magellan. This time I specify NO Money Line feature.

July 1986
Money is withdrawn from my checking account without warning. A statement shows up saying that the Magellan fund now has that money. I call Fidelity customer service and asked for this to stop.

October 1986
Money is again withdrawn from my checking account without warning. For the first time in my life my checking account is overdrawn because of this withdrawl. I am fined by the bank. I call Fidelity and ask them to stop. I write them a letter telling them to stop. I withdraw all my

money from Magellan. The beast should be dead. But .....

January 1987
Money is withdrawn from my checking account and placed into an otherwise empty Magellan fund account that still exists. This withdrawl causes a check to bounce for the first time in my life. I call Customer Service. They refer me to the Research Department. Research gets back to me later and assures me that everything will be stopped. TWO MONTHS later I get my money back. Meanwhile, I am fined by my bank for the bounced check and embarassed in front of the company I paid it to. Is the beast dead? Noooo ...

April 1987
Money is again withdrawn from my checking account without warning. The Money is put into a NEW Magellan account in my name. I transfer the money out. I visit the office of my bank where my account is. I ask them to cancel this connection to account. The flesh and blood people say they cannot help me and give me a phone to call Customer Service. Customer Service identifies the automatic debit feature on my account and puts a "STOP order" on it. The operator then says that she cannot guarantee that this will prevent the access from occurring again. She says that if the Fidelity computer asks for its money again, the bank computer will probably give the money to it. I'm furious. I complain to the flesh and blood people. They say there is nothing they can do.

Epilog
I am taking all of my money out of Fidelity to punish them for this and to avoid future problems with them. I will be cancelling my account with the bank and moving it somewhere else. Only then will I kill the beast. I hope ...
BIG BROTHER IS HERE AND HE IS A COMPUTER!!!

VCRs, Telephones, and Toasters

Martin Ewing <mse%Phobos.Caltech.Edu@DEImos.Caltech.Edu>
Wed, 22 Apr 87 23:15:07 PDT

I appreciate the comments of Beckman and Saltzer on inappropriate technology in VCRs, toasters, etc. I, too, have found it inordinately difficult to program our "7-day programmable" VCR.

The telephone offers another case. Our "Dimension/1" system happily takes a half dozen codes for call forwarding, camp-on, holding, etc., with zero feedback as to its internal state. Just for spite, it gives you a little chirp as you realize you forgot to reset call forwarding and your call has flown off to the other end of the building.

You can also get into exotic telephone situations with banks and mutual funds, as you can transfer five figures of cash between accounts without being *quite* sure afterwards what you have done.

A simple rule would be that any user interface should have visual output

that is in line with the complexity of the transaction. Visual because an entire transaction can be viewed at once. VCRs are lately using the TV screen for state indication, and financial institutions are providing PC access for their customers. Both are hopeful developments. I just don't know about smart toasters. Can they scorch ascii on your crumpets?

Martin

Checklists, Aircraft risks, and Neutrons

<eugene@ames-nas.arpa>
23 Apr 87 09:05:58 PST (Thu)

Subject: Re: Checklist stops risks?
From: Jerome H. Saltzer <Saltzer@ATHENA.MIT.EDU>

It seems maintenance is one of the biggest problems in software, and not uncommon to software. If there is any one area where we could use checklists, and where software people [and others] fall down, it is in the area of long-term maintenance.

From: ladkin@kestrel.ARPA (Peter Ladkin)
Subject: Aircraft risks
>One possible source of confusion - a blackout is not a loss of consciousness

The problem is there is a lag associated with loss of vision and loss of unconsciousness which does not travel at the speed of light. I would suggest it is not as easily reversed as implied. Better to stay far away.

Subject: Neutron beam detection [RISKS 4.75] (Scott Dorsey)
>In addition, what happens to digital electronics when they are hit with
>slow neutrons?

Yes, interesting indeed. You may have just justified the use of GaAs circuits for home use. This is especially critical when you consider we can sputter layers 20 atoms thick when hitting these atoms with neutrons.

--eugene miya, NASA Ames Research Center

Neutron Beams for Explosives Detection

Barbarisi <marco@ncsc.ARPA>
Thu, 23 Apr 87 16:29:25 CST

I did an experiment with neutron radiation for a physics laboratory while I was in college. It may shed some light on this issue.

For the experiment, a silver dime was placed in a device called a "neutron howitzer" and irradiated with neutrons for approximately one minute. The dime was removed and the gamma radiation emmisions were monitored. As I recall, the half-life of the radiation was about thirty

seconds (it was very "hot" upon removal from the howitzer). After about three or four minutes the gamma radiation decayed to background levels. The latex stick which held the dime in the neutron howitzer showed no sign of radiation at all.

Thus, I doubt that there would be any lasting effect on clothing and food from low energy neutron radiation. The device we used to irradiate the dime was in a refridgerator-sized can of lead and used plutonium to generate the neutrons. The device that is proposed for airport use is of considerably less power.

However, there would be considerable hazard to an airport worker stationed near the neutron emitter. I foresee lawsuits a-plenty when a baggage handler working near the bomb detector gets a nasty disease or produces afflicted offspring.

Marco C. Barbarisi marco@ncsc.ARPA (904)234-4954

Forgery on Usenet

<brad%looking%math%math.waterloo.edu@RELAY.CS.NET>
Wed Apr 22 19:07:34 1987

While I'm not sure we should be revealing all this, it is possible to go even further and make forgeries that can't even be traced by looking in the logs.

If you are root on your machine, you can change the machine's site name, so that it pretends to be another machine. If the remote site you are calling has a general uucp login, nothing prevents you from saying, "hi, I am site ihnp4, and here are some transactions."

cbosgd does have such a general login. If you insist on a different login (with password) for every network partner, than that can be safe IF you have a version of uucp that does security checks on the names.

I think lots of people have got secure uucp mail, at least within their organization, these days. I don't think they do with news.

Brad Templeton, Looking Glass Software Ltd. - Waterloo, Ontario 519/884-7473

Re: How to post a fake

<rti-sel!dg_rtp!throopw@mcnc.org>
Thu, 23 Apr 87 17:53:47 EST

> From: sun!plaid!chuq@seismo.CSS.GOV (Chuq Von Rospach) ...
> That's how you forge messages. And as long as the uucp links exist, there
> is no way to fix this, because a vital piece of information isn't passed out
> of uucp.

Well.... I disagree on a minor point. A news system could allow only user "news" to get at rnews, and only allow user "news" incomming access to uuxqt. (With perhaps similar arrangements for mail.) This means that uux would not be allowed for anything but news or mail, but it would plug the security hole. So, revise Chuq's point to be "as long as the uucp links on news systems need to be used for anything but news and mail, there is no way to fix this."

At least... I THINK so. Wayne Throop

[I am suppressing a bunch of other messages on this subject. It is important that you all be aware of the risks, although the nuances in trying to avoid them are probably beyond the interest of our readership community. Suffice it to say that most of the alleged solutions still have significant windows of vulnerability. PGN]

Search RISKS using swish-e

Report problems with the web pages to the maintainer

Search RISKS using swish-e

THE RISKS DIGEST

Forum on Risks to the Public in Computers and Related Systems

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

Volume 4: Issue 78

Sunday, 26 April 1987

Contents

Re: Fidelity Mutual Funds Money Line feature

Martin Ewing <mse%Phobos.Caltech.Edu@DEImos.Caltech.Edu>
Thu, 23 Apr 87 23:09:11 PDT

I'm another user of Fidelity's Money Line, and am now just a tad more nervous. This last horror story confirms my latent suspicions.

Fidelity EFTS transfers can be initiated automatically via their "FAST" telephone system. By calling an 800 number, and entering a sequence of some 20-30 digits, you can (1) get the status of your account (balance, last investment, redemption, and dividend), (2) transfer between two existing accounts, (3) transfer into a NEW account (in any of 60+ funds), and (4) initiate an EFTS transfer from your bank account (if preauthorized). Apparently all Fidelity accounts are born with FAST access. All you (or anyone else) need to commit fiscal mayhem are your Fidelity account number and a security code which (are you ready for this?) consists of the last 4 digits of your Social Security Number.

All of Salander's troubles might have come from a malicious "friend" on the telephone. Even without slurping up funds from the bank, such a prankster could create dozens of accounts for you in obscure funds. (Everything is

confirmed by mail, of course.)

I had thought that the 24-hr human assistance line would have been sufficient to correct any random computer errors. Their attitude has been good, in my experience. However, one particularly chatty operator did let on that, while she thought the FAST service was generally good, she strongly recommended calling the assistance line for transactions. "The computer line has no backup," she said.

I note that my discount brokerage is similarly lenient in telephone transactions. They don't have touchtone transactions, but they do take orders over the phone with only my account number and no independent verification. There outta be a law.

And now my bank has installed "TeleService" with features similar to Fidelity.

Re: Fidelity Mutual Funds Money Line feature

Brint Cooper <abc@BRL.ARPA>
Thu, 23 Apr 87 21:22:57 EDT

Thank you for sharing your story with us. But why didn't you handle the problem with the bank from the beginning? Around here, I don't think a bank can release funds except upon your authorization; and if you revoke that authorization, they may no longer release funds.

Then, upon occasion of the very first error, you simply close the bank account and withdraw all your money. Fidelity is left "holding the bag," as it were.

I hope that, by sharing our experiences with the risks of computer systems, we become more savvy at dealing with them. We're users as well as developers.

[I think we must all respond more forcefully when confronted with such human-caused and other computer horrors. Perhaps a Ralph Nader-like group might be appropriate, but individual action can also have an effect, especially in quantity -- carefully worded nasty letters, withdrawals of accounts, threats of lawsuits, and so on. PGN]

Re: Forgery on Usenet (Brad Templeton, RISKS DIGEST 4.77)

<mab@riacs.edu>
Fri, 24 Apr 87 07:32:12 -0800

Brad writes that there is no way to make USENET news secure, which is perfectly correct (as has been pointed out.) He goes on to say that "I think lots of people have got secure uucp mail, at least within their organization, these days." Sorry, 'taint so. First, on any BSD UNIX system except 4.3, and probably on any other UNIX V7-based system, mail on any machine can be trivially forged, because they all use the "getlogin()" routine to determine the sender. (4.3 does it right -- it uses "getpwuid(getuid())".) Look at that routine sometime -- it's one of the

easiest to spoof.

If you have an SMTP mailer, things get to be even more fun. SMTP does not do verification! Just connect to your SMTP mailer as would a foreign host, and you're off. (To test this, we forged a letter from Opus the Penguin at WhiteHouse.ARPA -- this was before domaining -- asking someone for pickled herring heads for lunch, but if none were handy, for anything but squid. Confused the heck out of the recipient until he asked the local mail guru, me, what happened.)

There is an effort by the Internet Advisory Board Task Force on Privacy to do something about protecting mail privacy and allowing it to be authenticated. The task force proposal will be transparent, so it can be dropped onto any SMTP implementation. If you're interested in this, grab a copy of RFC 989 from the NIC.

Matt Bishop

Re: VCRs, Telephones, and Toasters

<MJackson.Wbst@Xerox.COM>
24 Apr 87 11:04:11 EDT (Friday)

Perhaps this is all fallout from cost-effective technology in one area far outstripping advances in others? It is marvelously cheap to implement functions in silicon, but actuators and displays are still (relatively) expensive.

Thus one has the digital watch with 37 functions, each accessed by some unique manipulation of only four buttons. For the VCR, providing a screen display requires a (fairly inexpensive?) character generator, but what about for a (non-video) telephone?

From a human factors viewpoint the effective bandwidth of the interface limits the number of truly useful functions. But from a marketing viewpoint the ability to advertise a maximum number of (technically useful) functions is very attractive, and may carry the day. I suspect, therefore, that this is going to get worse before it gets better.

Mark

References on computer-professional certification

John Shore <epiwrl!shore@seismo.CSS.GOV>
24 Apr 87 10:00:54 EST (Fri)

I'm putting together a bibliography concerning the certification of computer professionals, and I would appreciate some help.

I would like references to material about

(a) pros and cons of certification

(b) efforts related to certification
(c) certification methods
(d) current practice in other fields
(e) history of certification in other fields

Depending on the length of the resulting bibliography, I'll either post it to RISKS or post an announcement about it.

Thanks in advance.

John Shore epiwrl!shore@seismo.css.gov ...seismo!epiwrl!shore

[We have noted previously the question of whether certification might help reduce risks resulting from human foibles during development, maintenance, etc. John's request is thus very relevant here. I look forward to the results! PGN]

Presentation on Star Wars Computing April 29, Chelmsford MA

Jon Reeves <reeves@decvax.dec.com>
Fri, 24 Apr 87 13:13:32 edt

"Reliability and Risk", a multiprojector presentation on the computational aspects of the Strategic Defense Initiative, will be given on Wednesday, April 29, 7:30p.m. at the Old Town Hall, in Chelmsford Center. Please forward this to anyone whom you feel would be interested. Thank you. --Joe

RELIABILITY AND RISK: COMPUTERS AND NUCLEAR WAR
A 34-minute slide/tape presentation

Reliability and Risk...
...investigates whether computer errors in key military systems--some of them unpreventable errors--could trigger an inadvertent nuclear war.

...features technical, political, and military experts discussing the role of computers at the heart of civilian and military systems, from the space shuttle to nuclear weapons to Star Wars;

...describes the ways in which all large, complex computer systems make mistakes--often unexpected and unpreventable mistakes:
- o The 46-cent computer chip failure that led to a high-priority military alert.
- o The software error that led to the destruction of the first Venus probe.
- o The design flaw that caused a missile early-warning computer to mistake the rising moon for a fleet of Soviet missiles.

...explores the growing reliance on computerized decision making and how a computer error could trigger a disaster, especially in a time of crisis.

...explains why we should not rely exclusively on computers to make critical, life-and-death decisions.

...uses straightforward language and graphics and is recommended for all audiences. No technical knowledge is required.

...received a Gold Award in the Association for Multi Image New England competition in November, 1986--the largest multi-image competition in the country.

Speakers in Reliability and Risk include:

o Lt. General James A. Abrahamson, Director, Strategic Defense Initiative Organization (SDIO)
o Lt. Col. Robert Bowman, Ph.D., US Air Force (retired), Former Director, Advanced Space Programs Development
o Dr. Robert S. Cooper, Former Director, Defense Advanced Research Projects Agency (DARPA)
o Dr. Arthur Macy Cox, Advisor to President Carter, SALT II Negotiations, and Director, American Committee on U.S.-Soviet Relations
o Admiral Noel Gaylor (retired), former Commander-in-Chief of the Pacific Fleet
o Dr. James Ionson, Director, SDIO Office of Innovative Science and Technology
o Severo Ornstein, Computer Scientist (retired) and Founder, Computer Professionals for Social Responsibility
o Professor David Parnas, Computer Scientist, Resigned from SDIO Panel on Computing in Support of Battle Management
o Dr. John Pike, Associate Director, Federation of American Scientists
o Dr. William Ury, Director, Harvard Nuclear Negotiation Project
o Actress Lee Grant as narrator
and many others

Reliability and Risk was produced by Interlock Media Associates and CPSR/Boston

Search RISKS using swish-e

THE RISKS DIGEST

Forum on Risks to the Public in Computers and Related Systems

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

Volume 4: Issue 79

Saturday, 2 May 1987

Contents

Risks of RISKS resurgent -- CSL DEAD FOR THREE DAYS, STILL HALF DEAD

Peter G. Neumann <NEUMANN@CSL.SRI.COM>
Sat 2 May 87 10:57:56-PDT

Somewhen on Tuesday afternoon, 28 April, someone plugged some equipment into the circuit used by CSL.SRI.COM. The result was not only blown fuses, but a physically destroyed disk on CSL. We currently have a patchwork system cannibalized from another system, with a very small disk, and thus I am running without most of my macros, history files, etc. (just the files created in the last month). We will not be back in regular service until the END OF THE COMING WEEK, so please bear with us. Mail received by RISKS after early Monday evening 27 April, but before the crash, was lost. Mail sent to RISKS by you during the outage was either returned undelivered, or else queued and eventually received, depending upon mailer whims. Grumble.

Re: Fidelity Mutual Funds Money Line feature (RISKS 4.78)

Amos Shapir <nsc!nsta!instable.ether!amos@Sun.COM>
Mon, 27 Apr 87 16:43:10+0300

Because of the slowness of mail here, the habit of paying your bills
by a 'permanent order' to your bank have become very popular; many
utilities also give discounts if you choose to pay your bills in that
way, since they are assured of getting their money - no bounced or bad checks.

However, a common experience is that it is very hard to cancel such an order -
you have to keep badgering the bank until your request gets all the way through
to the data processing center, and even when you think everything's ok someone
loads an old backup tape, and your stone rolls back to the bottom of the hill.

Sometimes the only way is to close the account, but when you have as many
as 10 such orders, that's also complicated.

Amos Shapir, National Semiconductor (Israel)
6 Maskit st. P.O.B. 3007, Herzlia 46104, Israel Tel. (972)52-522261
amos%nsta@nsc.com {hplabs,pyramid,sun,decwrl}

<minow%thundr.DEC@src.DEC.COM>
Mon, 27 Apr 87 06:02:42 PDT

(Martin Minow THUNDR::MINOW ML3-5/U26 223-9922 27-Apr-1987 0855)
To: "risks@csl.sri.com"@src.DEC.COM
Subject: Wheels up

You may recall the extensive discussion on Risks a few months ago
about computer-controlled airplanes. It seems, that if the plane was
on the ground and you told the computer to raise the landing wheels,
it did so -- crashing the plane.

I recently bought the "Flight Simulator" computer game for my home
computer. While parked on the ground, I told it to raise the (simulated)
landing wheels. It did so, crashing the (simulated) plane.

(If you haven't seen it, "Flight Simulator" is an impressive piece of work.)

Martin Minow minow%thundr.dec@decwrl.dec.com

Special Risk Assessment issue of 'Science'

Hoffman.es@Xerox.COM <Rodney Hoffman>
29 Apr 87 16:56:20 PDT (Wednesday)

Partial contents of 'Science' magazine for 17 April 1987 (vol 236 no 4799)

Editorial on "Immortality and Risk Assessment"
"Risk Assessment and Comparisons: An Introduction"
"Ranking Possible Carcinogenic Hazards"
"Perception of Risk"
"Risk Assessment in Environmental Policy-Making"
"Health and Safety Risk Analyses: Information for Better Decisions"
"The Safety Goals of the U.S. Nuclear Regulatory Commission"

[Computers are explicitly omitted. Eugene Miya]
[But there is still much for us to learn from this issue... PGN]

Radiation hazards to computers

Wm Brown III <Brown@GODZILLA.SCH.Symbolics.COM>
Thu, 30 Apr 87 17:42 PDT

Paul Stewart's contribution on airport luggage scanners which use slow neutrons to detect explosives reminded me of a phenomenon which plagued a company I once worked for. The product we sold was a satellite navigation receiver which used the old Transit constellation of satellites to provide position fixes for commercial ships. Many of these systems were sent around the world to be installed wherever a vessel happened to be at the time.

After a couple of years, we began to notice that our overseas dealers frequently had systems fail out of the box with invalid EPROM checksums. Machines installed within the U.S. virtually never failed in this way, even though they were built with parts from the same vendor and datecode lot. Spare PROM sets became a standard part of everyone's service kits.

Finally someone collected enough data to correlate these failures with the distance a system traveled by air freight; the dealers farthest from home usually saw the most failures. I seem to remember that flights over the polar routes did the most damage.

One of our engineers had a background in nuclear physics and power engineering; the best theory he was able to propose was that high energy particles in the upper atmosphere occasionally hit heavy metal atoms in the ceramic chip packages and kicked out slow secondary emissions which corrupted cells in the EPROMs.

Has anyone else had first-hand experience with this phenomenon? Can someone with adequate theoretical knowledge offer another hypothesis? Do the FAA's new bomb detectors pose a similar threat?

Neutron beam detection [RISKS 4.75]

Richard H. Lathrop <RICKL@OZ.AI.MIT.EDU>
Mon, 27 Apr 87 11:34 EDT

Date: Mon, 20-Apr-87 00:40:59 PDT

From: beach!paul@rand-unix.ARPA (Paul Stewart)
Subject: Radiation risk at airports?
To: risks@csl.sri.com

....a computer-based system that bombards luggage or other cargo with a "beam of slowed neutrons" and uses a computer system to analyze the signature of the resulting gamma radiation emissions to characterize for the potential presence of explosives.

I have been licensed by the US NRC as a nuclear reactor operator (I have since allowed this to expire), and was once the chief programmer and statistician on a science project which used this technique to monitor trace element pollution in tree rings. The method is known as Neutron Activation Analysis (NAA). It is based on the propensity of an atomic nucleus to absorb a neutron and thereby transition to another isotope of the same element, but with the next higher atomic weight. The resulting isotope is often energetically unstable, and often decays to a stable state by emitting a gamma ray at a frequency characteristic of the isotope involved. (This is a slightly different mechanism from the propensity of plutonium-239 and uranium-235 to absorb a neutron, become unstable, and fission.)

The neutron capture coefficient (known as the "cross-section") is a characteristic property of the elemental isotope, and can be looked up in tables of physical constants (e.g., the CRC Handbook of Chemistry and Physics), as can the stability, decay mode, frequency, and half-life of the resultant isotope(s). The cross-section varies widely across isotopes (a spread of ten orders of magnitude!). As some naturally occurring isotopes transition to other stable isotopes and some have miniscule cross-section, activated gamma radiation will result only in some (this means many) cases.

For short irradiation times the amount of any given isotope created is the product of the neutron flux (intensity), the time period irradiated, the amount of the element present, the proportion of the element occurring as the precursor isotope, and the precursor isotope's capture cross-section. (Note that if the flux is extremely low very little of the radioactive isotope will be created.) If the resulting isotope is unstable, it will emit radiation at a characteristic frequency and half-life, also obtainable from tables. The shorter the half-life the more intense the short-term radiation, the longer the half-life the longer the radioactive isotope persists. By measuring the radiation at a particular frequency of interest and subtracting the ambient background, it is possible to calculate the amount of a given element present in the original sample.

The question then, for anyone who understands this technology or knows about Science Applications International, is: what will happen to luggage, cargo, etc., possibly including foods and other items that can be ingested or will be in close proximity to persons for long periods of time, after passing through such neutron beam systems once or possibly many times in the course of complex or multiple trips?

Almost all of the above will become slightly radioactive, the degree to

which being essentially determined by the neutron flux characteristics, exposure times, and elemental content of the irradiated matter. Bodily damage from radiation results mostly from the accompanying ionization, in which chemical bonds are disrupted by the high energy levels and chemically reactive ions are created. Food is particularly worrisome because most of the radiation is absorbed internally, and because the body has mechanisms that produce high local concentrations of certain elements (e.g., iodine in the thyroid, calcium in the bones, etc.). Common isotopes in food having high natural abundance, reasonably large cross-sections, and medium half-lifes (hence, readily made radioactive) include sodium-23 and chlorine-37. Common metals with similar properties include aluminum-27, copper-63 and -65, zinc-64, silver-107 and -109, gold-197, mercury-202, and several of the trace elements used in making stainless steel.

> Are airline passengers to be subjected to the radioactive luggage and cargo simply because the emission levels meet "government standards"?

Well, yes, but this has to be kept in perspective. For example, "government standards" are typically less than the ambient background due to cosmic rays, etc., and also less than the incremental increase due to living in a brick house (because of trace radioactive elements and isotopes present in the brick from the earth), living in Denver instead of New York (because of the greater exposure to cosmic rays from less atmospheric shielding), or a medical X-ray. This does *not* mean that they are harmless --- the effects of low-level radiation are *very* poorly understood and the health aspects, if any, somewhat controversial. Of especial concern is genetic damage due to ionization and resulting disruption of chromosomes.

> Will the frequent traveler be at greater risk than the occasional traveler?

Yes, given the perspective about ``risk'' above.

> What is the real story about these systems?

I cannot answer this question, only discuss the underlying technology. The "real story" depends on (1) physical parameters such as exposure time and neutron flux characteristics which are not provided in the story, and (2) medical effects of low radiation levels, which are poorly understood and controversial.

> Date: Tue, 21 Apr 87 11:50:35 edt
> From: Scott Dorsey <kludge%gitpyr%gatech.gatech.edu@RELAY.CS.NET>
> Subject: Neutron beam detection [RISKS 4.75]
>
> A machine which detects nitrogen chains may also detect things like ammonia if it cannot discriminate between long and short chains....

For virtually all purposes nuclear processes are completely decoupled from chemical ones, and so the technique cannot discriminate between long and short chains. It is in fact unlikely that nitrogen is being detected in this way. 99.63% of natural nitrogen occurs as nitrogen-14,

which on neutron capture transitions to nitrogen-15 which is stable. 0.37% occurs as nitrogen-15, which has an insignificantly miniscule capture cross-section. This makes sense when you think about it, as otherwise the nitrogen in the air would render the technique worthless. Rather, it is more likely that some readily-activated rare-earth element associated in trace quantities with explosive manufacture is what is actually being detected. This is done, e.g., in studies which wish to monitor the lead deposition from gasoline even though lead is essentially inactivable. These studies look instead for vanadium, which occurs in gasoline in trace amounts but is readily activated and detected.

> Date: Thu, 23 Apr 87 16:29:25 CST
> From: marco@ncsc.ARPA (Barbarisi)
> To: risks@csl.sri.com
> Subject: Neutron Beams for Explosives Detection
>
> I did an experiment with neutron radiation for a physics laboratory while I was in college .... a silver dime was placed in a device called a "neutron howitzer" and irradiated .... it was very "hot" upon removal

As mentioned above, silver activates rather nicely. Typically this experiment measures the two different half-lives associated with the two different silver isotopes which are activated.

> The latex stick which held the dime in the neutron howitzer showed no sign of radiation at all.

Carbon, hydrogen, nitrogen and oxygen, the basic elements of complex carbohydrates and many polymers, are all essentially inactive under neutron irradiation. In any case, for a physics experiment the holder would be chosen to be inert, so as not to compromise the experiment with spurious radiation.

> Thus, I doubt that there would be any lasting effect on clothing and food from low energy neutron radiation.

This is not a justified assumption without additional technical substantiation. It depends critically on what elements are irradiated, for how long, and within how strong a neutron flux.

-=*=- Rick

Computer Database Blackmail by Telephone

Steve Summit <stevesu%copper.tek.com@RELAY.CS.NET>
Fri, 1 May 87 08:04:44 pdt

The following article was in the (Portland) Oregonian, 1 May 1987. I'm not quite sure what to make of it, except that I can't quite believe it. This looks like the kind of information abuse that people (myself included) would say "couldn't happen, because people are more reasonable than that."

PNB CANCELS 976 NUMBER FOR PERSONAL-DATA COMPANY

> Seattle (AP) -- Pacific Northwest Bell has canceled the 976-prefix toll-call number of a Seattle company that obtains and sells information about individuals. The company had sent post cards to thousands of Seattle residents, offering to delete data about them from company files if they called the telephone number--a call that cost $7.50. After PNB attorneys alleged that the post cards could involve extortion, the phone company canceled Profile Service Corp.'s 976 number Monday, the first time such action had been taken in the Seattle area, said PNB spokesman Bruce Amundson.
>
> But Jan Sakamoto, Profile's president, said the company did nothing wrong and would appeal the phone company's action to the Washington State Utilities and Transportation Commission. "I don't think it's blackmail or fraud," Sakamoto said. Instead, he said, his company was "catching the brunt of people's ire at not being able to control information about themselves."
>
> Commission spokesman Raymond Day said PNB apparently was within its rights in canceling the number. The commission allows PNB to cut off service "without prior notice, for unlawful use of service or use of service for unlawful purposes," Day said.
>
> Seattle news media, the state attorney general's office, the Utilities and Transportation Commission, the Postal Service and PNB have received numerous complaints about the cards, which were mailed to 20,000 Seattle residents. The card read: "Profile Service Corp. knows some personal things about you that other people might like to know. Our company's computer files contain names, telephone numbers, complete addresses, credit reports and other important pieces of information about you. We have purchased this information from a variety of public and private sources." The card then advised consumers to call its 976 number to have the number deleted from its computer files. The $7.50 charge for the call would be billed to caller's phone numbers, with most of the charge being remitted by PNB to Profile. People who called the number will have the charge deleted from their phone bills, Amundson said.

I think it's interesting that the company is not offering to delete information because it is incorrect, but simply because people might not want it there, as long as they are willing to pay. It would not surprise me if Profile Service Corp. didn't really have any data at all, but was simply out to milk money from people who are anxious about "not being able to control information about themselves."

It's refreshing that Pacific Northwest Bell chose to put a stop to this scam. I suppose they could have stayed out of it, saying it was Profile's business.

No mention is made of what "use" Profile Service Corp. makes of the data it keeps. If their raison d'etre is simply to get rich on people's $7.50 paranoia calls, they can preserve income, lower expenses and raise profits by not maintaining an expensive computer database at all. It would be interesting to know how big Profile Service Corp. is: if it's just Jan Sakamoto in his garage, and if he's got other income, he can't lose: the only expense is the postcard mailing, so once that is recovered, each phone call is pure profit.

Steve Summit

Liability Law in the UK

Brian Randell <brian%kelpie.newcastle.ac.uk@Cs.Ucl.AC.UK>
Wed, 29 Apr 87 11:05:46 bst

From Datalink (UK) March 23 1987:

LAW THREATENS FIRMS WITH COURT OVER FAULTS

A new Bill may leave computer companies wide open to claims for personal injury says Angus McCrone:

Software and hardware suppliers are being advised to take careful notice of a new law which means they could be sued for damages if their products are involved in a user's personal injury.

The law is a product liability bill which is now on its way through parliament and should be on the statued books by May next year.

The bill gives individuals the right to sue companies if they can claim that they have suffered personal injury as a result of defective products - whether computer products or any other sort.

This is likely to apply not only where an individual suffers injury from using a computer system, but also where a computer error is alleged to have caused an accident, such as a plane crash. Computer suppliers could even be sued if their systems have designed a large object, such as a bridge, which has fallen down and caused injury.

This marks a radical change from the past, when products suppliers were only likely to be sued for damages if it could be proved that they were guilty of clear negligence.

The proposed legislation has prompted groups like software's Computing Services Association (CSA) and hardware's Business Equipment Trade Association (Beta) to warn of serious consequences for their members.

Alan Smith, director of administration at Beta - which represents most of the big hardware manufacturers including IBM, ICL, Honeywell and Hewlett Packard - said that his organisation is 'very worried' about the new legislation.

"It completely reverses 500 years of legal precedents,' Smith said. 'At the moment a claimant has to prove negligence by a supplier and that this negligence was the cause of injury.

'In the future, as a result of this legislation, all suppliers will be treated as guilty unless they can prove that their products did not cause the injury.'

In other words, Smith reckons the difference between a system or program

going wrong, and being misused, could be blurred. 'If someone misuses a computer in the machine tool industry or in a hospital, who is to say that the system did not malfunction and cause the injury?'

He predicts that the product liability legislation would hit hardware vendors in two other respects - it will become much more difficult and expensive for them to insure products for liability, and they could be hit by a spate of 'spurious claims' for damages.

Both factors will present suppliers with increased costs. Smith said; 'The next five to 10 years could be a nasty experience for a lot of companies.'

But while hardware vendors look certain to be hit by the proposed product liability law, it is still not clear whether software will be included in the legislation or not.

Ranald Robertson, legal services manager at CAP and an expert on software and the law, commented that the Government has not made clear whether software will be treated as a 'product' and so will be covered by the new legislation.

Robertson said; 'Until a test case is brought to court, we are unlikely to have a definitive statement as to whether software is included in the legislation. 'But any software producer which ignores this legislation and its possible implications does so at its own peril, because there could be situations where a defect is attributable to faulty software and a potential liability could exist', Robertson added.

Doug Eyeions, director general of the CSA, described one example; 'If software is used to make a bridge or a nuclear reactor, and it turns out to have bugs, then this legislation could lead to an enormous liability for the software supplier.'

The CSA is arguing that software, by its very nature, cannot be guaranteed to be 100% bug free and cannot be tested in all possible circumstances - therefore it would be unfair to classify software as a 'product' for the purposes of the new law.

Another argument which the software industry is putting forward to the Government is the so-called 'development risk defence'.

This argues that a supplier should escape product liability if it is judged that with the benefit of current scientific knowledge, it could not have foreseen a particular defect.

But these sorts of arguments may fall on deaf ears. One parliamentary amendment which had the support of Beta has already been defeated.

The Government is also under pressure from the EEC which has issued a directive requiring all its member states to have suitable product liability laws in place by May 1988.

Because the proposed law applies to all products the implications for the software and hardware industries have taken some time to sink in.

But groups like the CSA and Beta are now lobbying very hard to influence what Eyeions describes as 'one of the major issues facing the industry'.

Elsewhere in the paper, a brief summary article states:

According to Praxis chairman Martyn Thomas, who is involved with the Alvey formal methods team, this could mean software houses will have to prove they used state-of-the-art formal methods in the design stage.

Rather than companies sorting themselves out in time for the new law, he thinks "what's more likely to happen is that there'll be a court decision that a company wouldn't have been liable if it had used formal methods.

Brian Randell - Computing Laboratory, University of Newcastle upon Tyne

UUCP : <UK>!ukc!cheviot!brian
JANET : brian@uk.ac.newcastle.cheviot

Search RISKS using swish-e

THE RISKS DIGEST

Forum on Risks to the Public in Computers and Related Systems

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

Volume 4: Issue 80

Tuesday, 5 May 1987

Contents

Computer Risks at the Department of Transportation

Peter G. Neumann <NEUMANN@CSL.SRI.COM>
Fri 1 May 87 17:02:08-PDT

In an editorial on page A.14 of the San Francisco Examiner and Chronicle on 26 April 1987 were some comments on air passenger complaints having doubled in March 1987 compared with March 1986. ``But the airlines weren't the only ones falling short in service. The Department of Transportation ... usually issues its complaint report monthly, but the one for March was the first since December. The delay was blamed on computer malfunction. Could it be that the Transportation Department has the same computer system as the airlines?'' [Hey, I'm just quoting. No responses please on whether the last sentence was facetious or whether the editorial writer is stupid. PGN]

The SF Chronicle on the following day had an article noting that air traffic controller errors at Chicago's O'Hare Airport increased 65% from 1985 to 1986, and nearly led to major disasters on several occasions. [From a newly released congressional report.]

The SF Chronicle on 28 April quoted National Transportation Safety Board Chairman Jim Burnett, that a forced reduction in the number of flights is a necessary short term step to offset the recent rise in air traffic

controller errors and near-collisions. FAA chief Donald Engen defended the system as safe and said that Burnett does not understand it. ``I don't believe we should adopt a policy of restricting air commerce in this country", he said.

Computerized advertising network used to fence hot circuits

Peter G. Neumann <NEUMANN@CSL.SRI.COM>
Tue 5 May 87 09:54:34-PDT

Richard Gaudet and William Gorgizian are accused of taking $250,000 worth of integrated circuits from a San Jose electronics company, setting up a phony parts-supply company, advertising through a nationwide computerized network, and distributing around the country (via UPS -- see next message). Along with $200,000 in computers and burglary tools, authorities also confiscated a book entitled "The Perfect Crime and How to Commit It".

EPROMS and "Wimpy" Energy Physics

Patrick Powell <papowell@umn-cs.arpa>
Sun, 3 May 87 19:52:14 CDT

You better believe that there is a problem shipping things via airfreight.

First, let me give you a glimpse into semiconductors, especially the (old) EPROM technology. (If you know this stuff, and disagree with my explanation, quit quibbling: you know what I mean). The way that an EPROM stores information is by "trapping" a bunch of charges in an "insulated" region; you can do the same thing by statically charging up some material, and not letting the charge drain off. This trapped charge can be used to modify the characteristics of a transistor: if the charge is not there, the transistor will turn on (off?) when asked to; otherwise it looks like a dead duck, and will not turn on or off. Let the "good" transistors represent a 1, the bad (trapped charge) a 0. VOILA! Programmable Memory... just find a way to get the charge there. Well, that can be done by placing a fairly high voltage across the transistor, which causes a strong electric field, which will BLAST those little charges into place. Hopefully. Sometimes you have to do this several times, i.e.- you have a programming cycle.

Well, all this depends on the charges staying there. Do you know what happens when a charged particle rips through a solid? It leaves a little chain of ionized atoms in its path; luckily this only lasts a short time. Zap! there is a conducting path, and away some of those little devils race, hither and yon. And you lost some charge. Do this often enough, and PRESTO. No more stored information.

Now at 20 Km up there (60,000 feet: 12 miles), you would be amazed at the numbers of highly energetic particles. Of course they will get "absorbed" by the atmosphere, but that is a Loooong ways down. One of the reasons why

military equipment is "Radiation Hardened".

By the way, it isn't just High Energy Particles. One of the interesting things is that UltraViolet light puts out enough OOMPH (highly technical physics term) to cause the charges to start leaking, and is how you can erase a EPROM. Well, ordinary light will also effect semiconductors, in a similar manner. In fact, enough light, and a "nonconducting" transistor will start conducting. Luckily all those transistors are hidden away inside little opaque packages, except for (are you ready?) EPROMS! which need a clear window so they can be erased.

So here we are, with a new system, on public display. The program was in EPROM, and was on a board. "Lets open the cabinet, and show people a running system!" This led to the main board, with it's EPROM, being exposed to the public gaze. And to their cameras. Flash Cameras. With BIG Pulse Zenon Bulbs. 10 Microsecond flash, 4 times light of sun blah blah. Flash! Flash!

...Parity Error! EPROM Parity Fault! Reset and Restart....

From the comments I heard, this just about drove a couple of people nuts.

By the way, if you want to see if this works, try getting one of those "singing cards" with the IC on it. Some of them have been potted in CLEAR jel, and you can actually see the chip. Get the thing singing away, and then shine a light on it. A strobe light works best, and you can actually hear the effect.

Patrick ("Hardware? If it was easy to build we'd call it Software!") Powell

---

Re: Wheels up (RISKS 4.79)

Richard M. Geiger <prls!mips!rmg@Sun.COM>
Mon, 4 May 87 20:19:59 PDT

I once saw a Cessna light plane with a prop which had severely curled-back blades. We asked the F.B.O. (employee of the rental company which owned it) what had happened. We were told that the plane was equipped with (overly-sensistive!) automatic landing gear retraction. It had hit a bump while taxiing, and bounced; the mechanism decided that the plane had taken off, and raised the gear. Didn't do the engine much good.

Rich Geiger {decvax,ucbvax,ihnp4}!decwrl!mips!rmg
MIPS Computer Systems, 930 E. Arques, Sunnyvale, CA 94086
(408) 720-1700 x308 [Day Job] (408) 739-7911 [home]

---

re: Wheels up

The Polymath <ames!hollombe@ttidca> <Jerry Hollombe>

Tue, 5 May 87 13:21:18 PDT

As a pilot and aircraft mechanic I can tell you this is not a realistic simulation. All aircraft with retractable gear have a safety switch (often called a "squat switch") that senses when any weight is on the landing gear and interrupts power to the retraction mechanism in that condition. Barring electrical/mechanical failure the gear will not retract while sitting on the ground.

A common but unsafe practice is to flip the gear control to "up" while taxiing and allow the gear to automatically retract as the plane lifts off.

The Polymath (aka: Jerry Hollombe, hollombe@TTI.COM)
Citicorp(+)TTI 3100 Ocean Park Blvd. (213) 450-9111, x2483
Santa Monica, CA 90405 {csun|philabs|psivax|trwrb}!ttidca!hollombe

---

Liability for software "unless you buy our method"

John Gilmore <hoptoad.UUCP!gnu@cgl.ucsf.edu>
Mon, 4 May 87 01:22:46 PDT

#define slime people /* For the squeamish */
Oho! The slime who are in business to tell you how to take risks ("pay us money to assume them") and have coerced the government(s) into making it illegal to do otherwise, are now joined by the slime who are in business to tell you how to build software ("pay us money to use our formal design software") and are now attempting to get government guns to enforce their methods too.

[Somewhat overstated, but certainly a risk! PGN]

Search RISKS using swish-e

THE RISKS DIGEST

Forum on Risks to the Public in Computers and Related Systems

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

Volume 4: Issue 81

Thursday, 7 April 1987

Contents

Cadillac to recall 57,000 for computer problem

Chuq Von Rospach <chuq@Sun.COM>
Wed, 6 May 87 08:49:01 PDT

I heard this on the radio coming in:

> Cadillac is recalling 57,000 84-86 cars for what they termed
> 'problems with the headlight computer that would cause your
> lights to go out unexpectedly'

Now, wouldn't THAT be fun. What I want to know is whether it is hardware or software.

[For reference, the GM car computer is the 68HC11, a custom CMOS chip based on the 6809 with lots of bit operations added in. They use two per car, one for the engine, and one for the body operations. Both are programmed exclusively in assembler.]

chuq

> [Presumably the two computers are totally independent and provide no redundancy -- with no possibility for alternate hosting or comparison.

Does it matter whether WHAT is in hardware or software? If the computer has to go back to Detroit for repairs, it doesn't matter. If your garage mechanic can download a new program it might, but then we get back to an earlier RISKS discussion about whether you will trust your mechanic to mess with your software... PGN]

Public E-Mail Risks?

<clapper@NADC>
7 May 1987 09:46:40-EDT

Excerpt from Federal Computer Week, Volume I, No. 6 (May 4, 1987):

Ecom Resurrected (by M. J. Richter)

The U.S. Postal Service's Electronic Computer-Originated Mail (Ecom) system, a short-lived and very unprofitable operation in the early 1980s, has risen from the ashes and will go into operation in the private sector this September. TCOM System Inc. ... plans to offer federal and commercial customers overnight to two-day mail delivery service via a data network. Laser printers will produce hard copies of messages sent over the network ... and the U.S. Postal Service will deliver the messages along with first class mail. ...

GTE Data Services of Tampa, Fla., just signed a five-year, $50-million contract to serve as TCOM's central processing and network management organization. Customers will send their computer mail over telephone lines to one of the GTE Data Services' nine processing centers.

At the data centers, the electronic mail messages will be sorted by ZIP code, furnished with ZIP+4 codes and then transmitted to one of 25 TCOM regional operating centers. There, the documents will be printed on high-speed laser printers, inserted by machine into envelopes and sent to the U.S. Postal Service for first class mail delivery. A full-page letter will cost 65 cents, and each additional page will cost five cents. ... TCOM trucks will transport the hard copies ... to regional post office hubs for delivery along with regular first-class mail. ...

The TCOM "enhanced mail-distribution" operation, slated to start up on Sept. 1, is an exact private replica of the Postal Service Ecom system that opened up in January 1982. ... At the time Ecom operations began, the Postal Service said more than 80 business organizations had signed up for the service, and that four telecommunications carriers had contracted to provide the electronic transmission portion of Ecom.

About two years later, protests by Congress and the Postal Service board of governors over Ecom's rising tide of red ink cause the Postal Service to discontinue the operation. ...

I'm wondering how secure this mail will be. While most computer "tech-ies" are aware that electronic mail isn't necessarily private, many non-technical

people don't consider or aren't aware of the susceptibility of electronic communications (especially electronic mail) to interception. Customers may well be mailing private or sensitive information (financial, personal, whatever), assuming it is as confidential as a traditional sealed-and-stamped letter. Should one of the stuffing machines or laser printers jam, presumably some human must un-jam it. What's to prevent him/her from casually reading the letter which was being processed? After all, if an open letter just falls into *your* lap, don't you usually read at least part of it? (Only to figure out what it is so you can return it, of course... :-))

Brian M. Clapper

[By the way, there were still more messages on spoofing mailers that are not included here. I think you all get the idea that spoofing is amazingly easy, and that most attempts to patch things up don't work. PGN]

Wheels up (and simulators) (RISKS DIGEST 4.80)

Eugene Miya <eugene@ames-nas.arpa>
Wed, 6 May 87 00:30:31 PDT

I had a local ACM/SIGGRAPH core (staff) meeting this evening. We will be having a special tour for our local members. A special demonstration was offered to us by Ron Reisman of Singer-Link at the Man-Vehicle Systems Research Facility (MVSRF). This facility was featured during the "why planes crash" episode of Nova and we "flew" in the two simulators shown on Nova.

The first, Advanced Cab, simulates a non-existent plane of 1995 with all the latest bells and whistles which are not flight certified: advanced CRTs, checklists (not paper), side sticks, etc. This system does not have a motion base and is about a $2M image generation facility, it was pointed out that the side stick alone costs $125K. The whole thing is multiples of $10M. Scene is a Link Night scene by a DIG (Digital Image Generator). We "took off from SFO" and flew thru the Transamerica Building. We reset the system, and I dropped the question on Ron. Just to let you know, the knobs of the system are human engineered, the flaps know look like little flaps, the landing gear gear looks like a little landing gear (I learned the story of this at JPL: to avoid similar looking knobs and pulling the wrong thing). So we pulled the landing gear while on the ground. Plane bounded up and down basically taking off: (oh yes, the engines were on, we have to specify the test conditions while pulling wheels up) not the wrong thing, but not the right thing (obviously), it's a non-existent plane so they never cared, they knew).

The second simulator was a Class 2 727 simulator. This simulator is probably the most advance simulator in Northern CA (so says Ron). We had a 727 pilot with us on this one. This simulator has a live motion base and we could not fly with it (against FAA regs). We have had injuries (broken arms) by unauthorized "flights" with a high turbulence setting: you have to be a real 727 pilot to use it. This is the real simulator used by Boeing trained pilots. The people (Ron and I can't remember the pilot's name [HER name BTW]) assured me that the 727 had

interlocks to prevent gear retraction while on the ground. Every eventuality of this type has "been taken care of." You can agree or disagree with this, but I hope you can see why we should not do this type of test in this machine. They were aware of the F-16 simulator problems. Just testing.

Basically, the MVSRF people thought the wheels up thing was a bit strange: probably an easily related over simple, but obvious example of problems. They are more concern about what makes plane crash: designs are written on paper with ink, checklists are written on paper with blood (Ron). They are worried about more subtle but complex problems. I think there is a bit of naive on both parts and would recommend suspending this line of discussion. If some one else gets a chance to try the the F-16 simulator at GD in the Mid-West, you might post, but the professionals of this area think we are knit picking.

--eugene miya, NASA Ames

Re: wheels up

Doug <Faunt@SPAR-20.ARPA>
Wed 6 May 87 12:17:38-PDT

I worked on A4's in the Navy, and we had a problem with the wheels up interlock circuitry, and people. There was an interlock so that the wheels could not be raised with weight on them, however, this interlock also disabled the radar altimeter. To test the altimeter, this interlock had to be defeated. The proper procedure was for one person to manually actuate the interlock switch, which was on one of the main landing gear, while the testing was going on. Since this would mean four people were required to test the unit, work-arounds were sought after by those of us on the line. One of these workarounds called for removing a fuse from a panel in the forward nose gear well while the test was in progress. Sometimes the fuse didn't get replaced, and didn't get noticed during preflight. This caused the up-and-locked indicator system to not indicate. This annoyed pilots. It never had any serious consequences that I knew of, but....

Re: Wheels Up

Matt Jaffe <jaffe%cf5.UCI.EDU@ROME.UCI.EDU>
Wed, 06 May 87 12:54:50 -0700

Many military aircraft have an override which permits the gear to be raised even when there is weight on the main mounts. There are circumstances where safety requres one to raise the gear while on the ground. A typical example is when the aircraft has run off the runway and is headed for uneven or soft terrain. Leaving the gear down may, depending on the aircraft and terrain, result in the aircraft flipping inverted on the ground. For both the aircraft and any personnel on board, that is generally worse than merely sliding along on the

fuselage. (There was a fatal accident here - Los Angeles - in the Sepulveda basin recently when a T-28 made an emergency landing on terrain that looked decent but was not quite good enough.)

The relevant question for design engineers is, of course, under what circumstances may system operators require overrides to defeat safety mechanisms and how difficult can the override operation be made to be (to prevent inadvertent activiation) before it becomes so difficult to operate in times of stress that it presents more of a safety hazard (because it consumes operator attention and effort under what are obviously already stressful conditions) than if it were it not present at all?

Re: the Marconi deaths (an update to RISKS-4.74)

Brian Randell <brian%kelpie.newcastle.ac.uk@Cs.Ucl.AC.UK>
Thu, 7 May 87 17:25:07 bst

> [The April 30 issue of Computer News (the magazine that ran alone with the story for months before the rest of the media noticed) carried the most complete summary I have seen to date. Here it is, slightly abridged. Brian]

DEFENCE DEATHS: THE FACTS BEHIND THE STORY

The mysterious deaths of two Marconi systems experts first reported in Computer News have sparked off intense speculation. Tony Collins clears up the confusion surrounding this baffling series of events:

Late last year, a Bristol coroner, Donald Hawkins, spoke of a possible 'James Bond' connection between the deaths of two computer experts involved in key underwater defence projects.

Since then the mysterious deaths of five other defence workers have come to light. In addition, another scientist has disappeared and a senior ICL employee is critically ill after an unexplained fall.

Most incidents have occurred after the men have successfully completed important projects or left one job for another.

Although there are police suspicions that many of them were depressed for different reasons, Computer News could establish no obvious motive for suicide in any of the cases.....

Four of the dead men were employees of the GEC group - three at Marconi and one at Easams. Two others worked at separate times at the Royal Military College of Science at Shrivenham.

A Computer News investigation has established that most of the men were involved in computer simulation, arguably the key which opens the door to some of Britain's most secret defence technology.....

Marconi is Britain's only torpedo supplier and was last year awarded the Ministry of Defence's largest weapons order - (pounds) 400m for advanced anti-submarine Sting Ray torpedoes. The Sting Ray's computer aided guidance system is so advanced it is being used in the development of Marconi's strategic defence initiative (SDI) programmes.

The Royal Military College at Shrivenham is also involved in a number of Britain's leading edge defence projects. The college develops new testing devices for the Ministry of Defence and is engaged as a sub-contractor to defence companies on research and development.....

All the men involved were ambitious and demonstrated a special ability in their particular field. Marconi employee Vimal Dajibhai, 24, found dead beneath the Clifton Suspension Bridge last August, was about to leave Marconi for a higher paid job.

Ashad Sharif, another London programmer found dead in Bristol, was about to take over the running of a department at Marconi's Stanmore headquarters.

David Sands, who died in March as his car loaded with two cans of petrol exploded into flames as it crashed into a disused cafe, had just returned from a family holiday in Venice to celebrate the ending of a three year command and control systems project for Marconi's sister company Easams.

Marconi Space Systems employee Victor Moore (46) had just finished work on infra-red satellites at Portsmouth when he was found dead from a drug overdose. His death is said to have instigated an MI5 investigation, the results of which will remain secret.

There is also a separate investigation into Marconi based at Portsmouth by the Ministry of Defence Serious Crime Squad.

Early this year, two lecturers on top secret projects died in separate 'accidents' of carbon monoxide poisoning. Both had recently returned from America and had conducted research at the Royal Military College in Shrivenham.

The first, Peter Peapell, a lecturer and underwater acoustics expert, was found dead under his car and the garage door was closed. Although an inquest returned a verdict of accidental death, police are unsure how the accident happened.....

Despite reports that Peapell had no connections with electronics or computers he had in fact written a book on basic computers. He also had a paper published on underwater acoustic emissions.

The second, Dr. John Brittan, a former computer science officer at the Royal Military College was also inexplicably found dead in his car this year. He too was involved in computer simulation.

A few weeks ago, Stuart Goody (23) a post graduate at the Royal Military College at Shrivenham was killed in Cyprus while on holiday. He died instantly when his hired car collided head on with a lorry. The lorry driver was said to be unhurt. At least one senior employee at the college considered that the death could be significant.

Avtar Singh-Gida, a researcher working on an important Ministry of Defence underwater project, disappeared just three weeks away from its successful completion.....

About two weeks ago, Robert Greenhalgh, a contracts manager at ICL's defence division at Winnersh near Reading, suffered multiple injuries after falling from a railway bridge on his way to work.....

The firm admitted he had been positively vetted and may have had access to secret UK and Nato data.....

After every death, police have given unofficial press briefings which provide journalists with plausible though unconfirmed explanations for the accidents or apparent suicides.

The major problem for police has been the lack of obvious signs of depression in any of the cases.....

Several MPs have demanded a government inquiry although there are no signs that ministers will agree.

The answer to the mystery may never be known, at least in the short term. As one policeman said: "We'll probably know all the answers when the papers are released in 30 years time."

Search RISKS using swish-e

THE RISKS DIGEST

Forum on Risks to the Public in Computers and Related Systems

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

Volume 4: Issue 82

Sunday, 10 May 1987

Contents

Information Age Commission legislation in the works?

Peter G. Neumann <NEUMANN@CSL.SRI.COM>
Sun 10 May 87 18:41:52-PDT

The Information Age Commission Act is intended to ``create a forum for discussions and targeted research on the present and future impact of computer and communication systems on our nation and its citizens.'' This year's bill, S.786, is causing a lively controversy. Sponsors are Senators Sam Nunn (D-GA) and Frank R. Lautenberg (D-NJ). (Last year's bill passed the Senate, but did not make it through the House.) Apparently most industry trade associations (except ADAPSO) are lining up against it. Some think that if such a commission must exist, then it should represent industry views only. The view of your RISKS moderator (unofficially, of course, especially since RISKS does not pretend to speak offically for the ACM) is that such a commission COULD be wonderful -- if it is not a case of the fox watching the chicken coops, and if it does not become a bureaucratic tarpit. Otherwise it could be a disaster.

There is much background on the issues in an article by Willie Schatz in Datamation, 1 May 87, pp. 32,37,38,40, which quotes a CBEMA issue

paper saying ``there is no specific or even identifiable need, purpose, or focus for this commission, that it would be a government commission in search of a mission. The paper also contends that the commission could become a forum for "promoting sensational but unfounded allegations about the societal effects of modern information technology. The commission would needlessly provide a highly visible forum for those who retard the information age." ''

[Side note to Herb Lin: Herb, have you ever shown Senators Nunn and Lautenberg copies of OUR RISKS Forum??? Are we retarding (or retarded?) PGN]

Another computer taken hostage

Joe Morris (jcmorris@mitre.arpa) <jcmorris@mitre.ARPA>
Sun, 10 May 87 13:38:30 EDT

From the Washington Post, Sunday 10 May 87:

> FIRM, EX-OFFICIAL AT LEGAL LOGGERHEADS

> Lakeland, Fla. -- The former chief financial officer at an insurance company
> is holding the firm's computer files hostage with a coded password known only
> to himself, a lawsuit charges.

> Golden Eagle Group Ltd. wants a judge to order George C. Coker, Jr. to reveal
> the password he programmed a week ago into the company's computer, which
> Golden Eagle says contains current accounting in excess of $400,000 and
> extensive background data.

> Coker contends that certain computer files are his property and says he will
> reveal the password only if allowed to keep an IBM personal computer, which
> he said was given to him in exchange for working overtime, plus his last
> paycheck, a letter of reference and a $100 fee.

That's the entire article, verbatim unless I've missed a typo. It doesn't say anything about the size of the company, whether there had been any warning about disputes between Coker and the company, or any other data we could use to figure out what measures should have been taken to answer the risk which is now visible. I suspect, however, that the RISK question is in the same class as one I have never been able to answer for myself: at what point is it appropriate to trust a single individual in a process, as opposed to the cost of never letting one person do anything without another qualified person present? Should graveyard shifts with a single operator be prohibited? Should I double the number of system programmers in my shop so that no programmer ever does anything alone? There's no question about the risk such situations cause; the question involves the economic penalties of reducing the risk.

For that matter, the article doesn't say if the data is from a mainframe or a micro. How do you handle a no-solo policy on a personal computer?

And note that audit trails wouldn't help here; there's no question about who did what to the system. Offsite backups might help, but (a) Coker might have been in a position to sabotage them, and (b) if the data is more current than the backups, they're worthless. Let's see a show of hands of RISK-readers who can swear that all data in their systems (mainframe AND micro, please) is currently backed up off-site...on second thought, forget it.

Larceny OF Computers, not BY Computers

Systems Consultant; DTN 297-4445 <kaiser%renko.DEC@decwrl.DEC.COM>
08-May-1987 0837

A few days ago a computer seems to have been stolen from a laboratory I know of. It can't have been difficult to steal; it was a MicroVAX 2000, and if you haven't seen one, they're 5.5" x 11.25" x 12.75", small enough to fit in an athletic bag or a sample case. I know; I've done it.

It's not known yet, of course, who took the machine, but it is known precisely when it happened, because the machine was a member of a local area VAXcluster whose boot member (home base, with the system disk, etc.) was elsewhere on the Ethernet in another, better-secured laboratory; and when the MicroVAX 2000 was turned off, its absence from the cluster was immediately registered by the boot member.

Hmm. Does RISKS cover risks TO computers? Pete
Kaiser%renko.dec@decwrl.dec.com decwrl!renko.dec.com!kaiser
DEC, 2 Iron Way (MRO3-3/G20), Marlboro MA 01752 617-467-4445

> [Sure, why not? If a computer is stolen while involved in a critical application, that is part of the system risk... PGN]

Risks of superconductivity

<eugene@ames-nas.arpa>
08 May 87 10:47:54 PDT (Fri)

The current issue of TIME has two articles of interest: the smaller is the battle of the "hard" versus "soft" scientists with Serge Lang in one corner and Herbert Simon {indirectly} in another. I tend to side with Lang in this case.

The cover story is about recent advances in superconductivity. I am surprised that RISKS has not jumped on this topical band-wagon. I note some interesting things in the omission (since we have had the argument that the omission of computers we have regarded is a RISK).

1) computers were probably not used.

1a) If computers had been used could we not have had superconductivity sooner? Could not people have been "saved" sooner if higher-temp superconductivity was around sooner?

{I doubt it and so does PGN.}

1b) Is this a sin of omission of computers? {Probably not since there is more to understanding this universe than what is simulated on computers.}

2) The use of the word "tinkering" was prominent. I know Peter Denning does not regard tinkering as experimentation. The theory around superconductivity is poorly understood. Perhaps, physics should do less tinkering. 8-)

3) What are the risks to superconductivity? Don't higher speed trains means higher speed train crashes? (Ah yes, but the benefits outweigh the risks...) The computer science people worry, but this does not stop the physicists. What about all that LN2 out there? Will there be increased cases of frostbite? 8-) (Assuming we don't make room-temperature.)

4) A social commentary about the rate of technological change was made regarding the Super Collider (the SSC). Should that project wait or should it proceed? Similarly, should computing people jump on the superconductor bandwagon? Only ETA systems has LN2 cooled computer systems on the market. I think the reality is that we won't see this material in the computing arena for about 20 years because a) a lot of effort will have to be made to determine whether room temperature materials exists and b) that waiting will delay use of the current material (whether a) works or not): just like waiting for a better computer. Oh, on the 20 year time frame, the question is could existing computers shorten that time frame?

One more thought: I'm surprised there was no RISKy commentary on Fred Brooks "Silver Bullet" article.

--eugene miya, NASA Ames

UK Liability Law (follow-up)

Brian Randell <brian%kelpie.newcastle.ac.uk@Cs.Ucl.AC.UK>
Fri, 8 May 87 17:39:38 bst

The item I sent in recently from Datalink (of March 23) about proposed new Product Liability legislation in the UK contained a brief quote fromn Martyn Thomas (Chairman of Praxis, a UK software house) which gave an over-simplified view of his, and his company's, attitude to the use of formal methods. I therefore thought it only fair to pass on a slightly fuller quote from a letter by Thomas which appeared in the May 4 issue:

> "There are many mistaken views of formal methods, born from fear and ignorance. Formal methods are no panacea. Their use does not guarantee error-free systems. They are intended to make reviewing and testing easier, not to make such activities unnecessary ... if a software developer chooses to write down an important requirement or design decision using an imprecise language, when a precise one is readily available, then he has acted unprofessionally. If someone suffers damage as a result of that unprofessional act, it is right that they should be compensated. Customers whose life or business depends on their computer systems working correctly

will increasingly want the assurance that their software developers are applying the best available methods. In many cases, this will include the rigorous use of formal methods."

I can readily accept such comments - what concerns me is whether it will ever be possible to make reasoned judgements about the risks attendant on using a given complex program, and about how best to apportion resources amongst the various different techniques, such as verification, testing and the use of design redundancy, which might assist in achieving some given required level of reliability from the program.

Brian Randell - Computing Laboratory, University of Newcastle upon Tyne

UUCP : <UK>!ukc!cheviot!brian JANET : brian@uk.ac.newcastle.cheviot

Re: the Marconi deaths - an interesting fictional treatment

Jon Jacky <jon@june.cs.washington.edu>
Fri, 08 May 87 09:13:25 PDT

I recommend the novel, THE WHISTLE BLOWER, by John Hale. The plot concerns a British computer specialist who dies in an unlikely accident. Much better written than the usual thriller - really transcends the genre, as the critics like to say.

Sorry, I don't have the publisher, I returned the book to the public library a few weeks ago, but it seems it was a U.S. reprint of a novel originally published in the U.K.

- Jon Jacky, University of Washington

Search RISKS using swish-e

THE RISKS DIGEST

Forum on Risks to the Public in Computers and Related Systems

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

Volume 4: Issue 83

Tuesday, 12 May 1987

Contents

Risks of sharing RISKS

<TMPLee@DOCKMASTER.ARPA>
Mon, 11 May 87 10:39 EDT

In the last issue PGN asked if someone had shown previous issues of RISKS to a couple of senators drafting legislation. This treads on the boundary of inappropriate and risky in itself use of this medium. It is generally understood, I thought, that this kind of forum is private to its readers, although the larger the subscriber list the harder it is to maintain that fiction. Although I don't contribute much here, had I known there was a

likelihood that what I wrote might end up in the Congressional Record I'm not sure I would have contributed it -- how do others think, or can our moderator state what he thinks the policy is?

Ted

[Interesting question. We agreed way back in Volume 1 or 2 that material in RISKS was open for noncommercial redistribution, as long as that did not violate any explicitly stated caveats or copyright limitations. It is important to keep RISKS informal and unencumbered by red tape. Besides, IDEAS HAVE NO BOUNDARIES (except in closed minds). One of the main purposes of RISKS is to disseminate ideas and awareness.

My question to Herb (who is on leave from MIT, deeply embroiled in the legislative process) was sort of a bemused wonderment as to whether the proposed legislation had in any way been influenced by the existence of the RISKS Forum, since some of the goals are quite similar... PGN]

Information Commission

<JPAnderson@DOCKMASTER.ARPA>
Mon, 11 May 87 17:36 EDT

Peter, I am sorely troubled by the prospect of our Congress providing 'oversight' or whatever it is they do down there to our industry. Even in areas where they have a clear mission and even one might expect some expertise, the attention span of the Congress is measured in Microseconds between headlines. You will recall that last year, the Congress created and then jumped on the bandwagon of war on drugs. To my local knowledge, there has been no *action* in that war since. [I do recall the House passing a bill calling for some $400 Million to be spent on that war, but was saved from any notion of accountability by the Gramm-Rudman act or some such.] I really do worry about the grandstanding that such a commission would engender, and the sycophantic interaction between the congresspeople and an uniformed, shoot-from-the-hip press. Really a bad idea.

Cheers, Jim

[I noted in my comments that there are many pitfalls in the proposed legislation. But, an implication of what you say is very depressing: the difficulties of government are so great that meaningful oversight is almost impossible anyway. The fox shouldn't watch the chickens; the chickens can't watch the chickens; even the computers can't be trusted to watch the chickens. So what do we do -- throw out the chickens with the egg water? PGN]

``How a Computer Hacker Raided the Customs Service''

Peter G. Neumann <NEUMANN@CSL.SRI.COM>
Tue 12 May 87 00:10:54-PDT

Last year two radar-equipped planes that had been promised to Customs were

given to the Coast Guard instead as a result of late-night Senate actions on the federal budget. Customs Commissioner William von Raab then promised Coast Guard Commandant Paul A Yost Jr. that Customs would provide $8M in reparations to help the CG's airborne drug interdiction problem. But Senator Dennis DeConcini (D-AZ) told von Raab not to transfer the money, and to wait for the appropriations process instead. The Coast Guard decided to act on its own. Somehow acquiring Customs' computer account numbers, they simply caused $8M to be transferred from the Customs account to the CG account. To make a long story short, there were protests from Customs, and just as mysteriously as the money disappeared, it reappeared (although in two increments).

> [I adapted this from the Washington Post National Weekly, 18 May 87, p.34, thanks to Michael Melliar-Smith. Perhaps the HACKER was really a Coast Guard CUTTER (or was he a CONS CAR'd CDR (LISPing to starboard?) Just think what could be done in reprogramming government funds! PGN]

Computer thefts (re: RISKS-4.82)

Jerome H. Saltzer <Saltzer@ATHENA.MIT.EDU>
Mon, 11 May 87 11:21:38 EDT

At Project Athena for some time we've been trying to convince our vendors that if they hope to sell personal workstations worth $2K or more to students they are going to have to include in the physical design a top-to-bottom hole that penetrates the major box covers and the mother board, suitable for dropping a bicycle lock through, so that the machine can be chained to a dorm-room or apartment radiator, or a desk in an office. The reaction so far has been uproarious laughter (and several reports of newly-designed compact workstations stolen from one of the vendors).

Jerry

Bomb Detection by Nuclear Radiation (RISKS-4.79)

Michael Newbery <ubc-vision!calgary!vuwcomp!newbery@seismo.CSS.GOV>
11 May 87 02:22:08 GMT

Some years ago, the Ariande column in New Scientist proposed a novel and, as usual (?), unworkable (??) bomb 'detector'. You zap your 'bomb' with radiation of a flavour selectively absorbed by Mercury (but not otherwise strong enough to hurt.) The Mercury gets a little agitated by this and, if it happens to be part of Fulminate of Mercury, an explosion occurs.
So, you just march your passengers and their luggage, one at a time, down a bomb-proof tunnel and if they DON't go boom, let them on board. Even if they do have explosives/bullets they can't set them off without a detonator.
Unless they use Lead Azide.
Or carry little bottles of nitro-glycerine, or...

Michael Newbery, Comp Sci, Victoria Univ, Wellington, New Zealand
ACSnet: newbery@vuwcomp.nz UUCP: {ubc-vision,alberta}!calgary!vuwcomp!newbery

[All kidding azide, this is another of our classical unsolvabled problems. Technology cannot provide 100% guarantees. It also transforms the technology it is trying to protect against. Heisenberg strikes again, with a longer time constant. PGN]

Computer floods summer course registration at U. of Central Florida

"Mark Becker" <Cent.Mbeck%OZ.AI.MIT.EDU@XX.LCS.MIT.EDU>
Mon 11 May 87 22:59:41-EDT

"SNAFU ENDS HAPPILY AT UCF AS STUDENTS GET EVERY CLASS THEY WANTED"
by Laura Ost, The Orlando Sentinal, Saturday, May 9, 1987, Page D-3

[Reproduced with permission]

Thanks to a computer snafu, a nightmare for University of Central Florida students has turned into a dream.

UCF's new computer system failed to cut off pre-registration for summer classes as they filled. The happy result for students who often wait years to take required courses: They got everything they wanted.

At first, the glitch meant that 56 courses overflowed, and 700 of 8,000 spring students who pre-registered were in danger of being tossed out of classes they planned on.

But after discovering the problem April 24, officials decided there was only one answer: Give them what they want.

"From the student standpoint, it turned out splendiferous," UCF spokesman Dean McFall said Friday.

The solution was to add more than 40 class sections in education, engineering, and arts and sciences, and to extend employment of part-time and nine-month faculty members who want summer work.

The worst case was a speech course required for students without community college degrees. More than 300 signed up for three sections with a total capacity of 84. So, eight sections were added.

The expanded schedule is a big relief for students; some courses have had long waiting lists, meaning that students often had to delay required freshman courses until their senior year. Solving the registration problems wiped out the backlog.

"It showed us the full market for those courses," said Charlie Micarelli, vice president for undergraduate studies. "For the first time we could see the number of courses needed. It was kind of overwhelming... So there's nothing bad that doesn't bring out some good."

This was UCF's first use of the new computer system and the

software that operates it. The software was developed by the Florida Board of Regents technical staff, which uses UCF as a testing ground for the state university system.

The malfunctioning software was repaired in time for regular registration Wednesday, officials said. Classes began Thursday.

Provost Richard Astro said the expanded summer schedule won't cost extra because it eliminates the need for some classes next academic year. He said the university usually has enough regular staff members to cover summer classes.

"What you don't want to do is put an ad in the paper and say, 'Anybody who can teach, come on in'," Astro said. "Basically what we're saying [to regular staff] is 'Hey, do you want to work this summer?'"

A password-breaking program

Dean Pentcheff <dean%violet.Berkeley.EDU@berkeley.edu>
Mon, 11 May 87 21:24:45 PDT

A few days ago on our university UNIX system (4.3BSD), a friend of mine received the message reprinted below. Very briefly, someone seems to have cracked the passwords in the "passwd" file and sent a piece of warning mail to all the users whose password he cracked. Note that my friend's password was a dictionary word, while mine (uncracked) was a proper name beginning with a capital letter.

> To: xxxxxx
> Subject: A matter of security..
>
> Your password: zzzzzzz [correctly stated]
>
> As an experiment, and something of an unofficial public service, I
> have been experimenting with a password breaking program that was
> recently released into the public domain. Since anyone can use this
> program now, I thought I'd run it on violet's password file to see
> which passwords could be broken. Yours was one of them. If you're
> security conscious, or just don't like the idea of your password
> being so easily broken, then I would advise that you change it to
> a word not found in the english dictionary, or use a combination of
> upper and lower case letters. Either of these methods will render
> your password fairly invulnerable to attack..
>
> Yyyyyyyyy Yyyyyyyy

[I thought using the SALT offset was standard by now! Ho hum, another lesson ignored. So, we run it ONE MORE TIME here. PGN]

Sidelight on the Marconi Deaths

"Lindsay F. Marshall" <lindsay%kelpie.newcastle.ac.uk@Cs.Ucl.AC.UK>
Mon, 11 May 87 16:07:33 bst

According to one of my colleagues who has just returned from a visit to Italy, the Marconi deaths are in all the papers, and many of his friends were worried about him returning to the UK as his life must be at risk because he works in Computer Science research...

Date: Mon, 11 May 87 11:37:09 PDT
From: Dave Benson <benson%cs1.wsu.edu@RELAY.CS.NET>
To: risks%csl.sri.com@RELAY.CS.NET
Subject: Software Reliability book

Software Reliability: Measurement, Prediction, Application,
by J. Musa, A. Iannino and K. Okumoto (McGraw-Hill Book Co., NY, 1987),
is now available. I cannot contain my enthusiasm for this well-organized,
thoughtful, thought-provoking, well-written, [accolades]* book. A sample
from 7.4.3 Measuring Ultrahigh Reliability, Case Study 7.1 on Nuclear
Power computer-based monitoring system:

> ...we are 95 percent certain that at least ... 3 more (failures)
> will occur at some time. The ... failure intensity in 0.895/1000 yr
> (of computer operation) using the logarithmic Poisson model.

Yes, that's less than one software failure per millenium of operation.

The point is that these three AT&T Bell researchers have an excellent collection of methods for measuring and predicting software reliability, and have made these techniques easily accessable in this supurb book.

"The Whistle Blower"

Jeff Mogul <mogul@shasta.stanford.edu>
11 May 1987 1113-PDT (Monday)

Stanford's on-line library catalog made short work of finding this:

AUTHOR: Hale, John.
TITLE: The whistle blower / John Hale.
IMPRINT: 1st American ed. New York : Atheneum, 1985, c1984. 239 pp.; 23 cm.
LOCATION: PR6058.A438W5 1985: Green Stacks
NOTES: Item CSUG85-B26608 (Books) Language: eng Year: 1985

Search RISKS using swish-e

Search RISKS using swish-e

THE RISKS DIGEST

Forum on Risks to the Public in Computers and Related Systems

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

Volume 4: Issue 84

Tuesday, 12 May 1987

Contents

Information Age Commission legislation in the works?

<LIN@XX.LCS.MIT.EDU>
Tue, 12 May 1987 22:45 EDT

> [Side note to Herb Lin: Herb, have you ever shown Senators Nunn and Lautenberg copies of OUR RISKS Forum??? Are we retarding (or retarded?) PGN]

No. I work on the House side, rather than the Senate. I have suggested various points of contact in the House to people on software related issues, though.

In response to another question, In general, I would not have qualms about showing a hard copy of RISKS to anyone, since it is a public forum. In fact, I would bet that Lautenberg probably has access to

RISKS himself if he wants it, since he owns a large DP company.

[On your first paragraph, I was naively assuming that House and Senate people -- particularly at the staff level -- might actually speak with one another now and then... PGN]

Re: RISKS information sharing

Richard A. Cowan <COWAN@XX.LCS.MIT.EDU>
Tue 12 May 87 22:31:37-EDT

Given that the RISKS digest is distributed to hundreds, or even thousands of people on a computer network that is funded, for the most part, with public funds, I think contributors should consider their messages to be public. Certainly, the messages sent on RISKS can be monitored secretly by government intelligence organizations; I would think that it would be less of a concern if those messages were monitored by Congress.

As for the prospect that RISKS submissions might appear in the Congressional Record, I would doubt it. Quotes attributed to individuals must be documented, and I would guess that the electronic medium does not provide sufficient proof of the authenticity of a message. This is just a guess from personal experience; I sent a letter to Proxmire's office last year on computers and Star Wars, and I was asked a week later to send a SECOND letter giving them permission to use my letter in congressional testimony.

Rich

Risk of contributing to RISKS

"ESTELL ROBERT G" <estell@nwc-143b.arpa>
12 May 87 08:18:00 GMT+492:48

I've always assumed that "someone up there" [in DC] was probably reading everything we share on ALL the journals on ARPANET and its cousins [DDN, EDU, COM, etc.]. I think that's a fair condition of use of a resource that's funded by public taxes.

Indeed, I've often HOPED that Washington [and other] government leaders in each branch, especially in several agencies of the Executive branch, read some of these journals - and then thought about what they've read.

I think Ted Lee's concern is common enough; I know I've often rewritten submissions, trying to "walk on eggs" to share a truth [as I see it] that others [including perhaps my colleagues in DoD] may find unpleasant. That's why so many of my notes end with a caveat: "The opinions herein are mine alone, and may not be shared by any other person or organization, real or imaginary."

The other side of this concern is that often some frustration shows through in submissions to RISKS [and Arms-D, et al]; because the writers have tried to share some knowledge or wisdom, and have been ignored. So, just when we think

we're only "among friends" is the very time that "big brother" decides to pay attention. Murphy predicted that. I've often said that "The ears have walls, and the walls have ears."

Bob

Distribution of RISKS Digest to Congress

David LaGrone <LAGRONE%eg.ti.com@RELAY.CS.NET>
Tue, 12 May 87 08:15 CDT

I vote "DO IT!!". God only knows (and s/he isn't sure) who gets copies of computer bulletin board material, anyway. Besides, I think that the purpose and intent of THIS digest is right-hearted enough for distribution to whomever would benefit from its contents. And I would hope the purpose and intent of the contributors is equally right-hearted.

...Regards...David LaGrone

[Disclaimer: The opinions expressed by me are mine and not necessarily those of Texas Instruments, Inc., its other employees, their families, relatives, friends, business associates, my relatives, my friends, or anyone else I know or have ever heard of.]

<Michael Wagner +49 228 303 245>
Tue, 12 May 87 17:55 CET

<WAGNER%DBNGMD21.BITNET@wiscvm.wisc.edu>
Subject: Re: Information Commission (RISKS-4.83)

In issue 4.83 of RISKS, JPAnderson@DOCKMASTER.ARPA wrote

> ... an uniformed, shoot-from-the-hip press.
> ^^^^^^^^^

This got by the (usually good) editorial pen of the moderator. I assume that the intended word was 'uninformed'. I was long into the next sentence before I realized that I had a parsing problem. While 'uniformed' is a word, I don't really know what a 'uniformed press' would be.

The hint I used to correct my misunderstanding of this phrase was a pronunciation clue. If the author had intended to write "uniformed", he probably would have written 'a uniformed ... press' rather than 'an ...'. At least, that's how a Canadian (me) would say it.

Now how would you teach a spelling checker that? Michael

[Not Canadian, but California English? -- "(me) would say it", "him and her are going", etc. I won't press the point -- or any uniforms, either -- because I know the press is not uniform. PGN]

Information Age Commission; Summer Courses at UCF

Wm Brown III <Brown@GODZILLA.SCH.Symbolics.COM>
Tue, 12 May 87 17:56 PDT

In response to Ted Lee and Jim Anderson, I think it is inevitable that the government will sooner or later promulgate regulations for our industry; it is the basic nature of governments to do so. The more important questions are which branch(es) of government, what kind of regulations, etc. Personally, I'd rather see an open body such as Congress writing the rules, rather than some alphabet soup department (IRS, NSA, FBI) that would be much harder to fight. Congress at least listens to all sorts of inputs, including individuals, companies, PACs, and expert testimony. An agency generally writes rules to suit its own ends, and has lots of ways to discourage inputs that serve other interests.

There are some potentially useful things government *could* do for us, such as making net hacking and unauthorized disclosure of personal files criminal offenses or making liability limitations reasonable and predictable. We also need friends to help control the (mis)use of computers by government agencies, particularly in the area of law enforcement. Left to their own, I'm certain that some enforcement types would love to create a big-brother situation by creating huge databases with no controls on their access. The only body which can realistically offer protection against such abuses is a more powerful government agency, such as Congress.

If this forum can be used as a vehicle to enlighten our lawmakers, even to the minimal extent of making them aware of that the issues exist, I am all in favor of sending each congressperson a gift subscription to every issue. When topics like computer privacy and liability become the issue of the day (and they will, probably through some scandal or major screw-up), those of us outside of government will need all of the connections and communications channels we can find to make ourselves heard.

= =

Regarding Mark Becker on summer course registration at U. of Central Florida:

When I was attending the same institution (it was then Florida Technological U) about ten years ago, the first night of registration one quarter turned into a fiasco because it took *MINUTES* for the computer system to process each registration form. As it turned out, their new registration software had been brought on line without any live testing whatever.

The killer was that the program had been developed using an ordinary job control card with relatively low priority. Nobody thought to bump the priority level up when it came time to run live students (thousands of us) through the system, so the program was still running as a background task. To make matters worse, it turned out that the accounting department was running a massive batch job at that time of the evening, and they *HAD* thought to give their job the highest system priority they could get.

A password-breaking program

Dean Pentcheff <dean%violet.Berkeley.EDU@BERKELEY.EDU>
Tue, 12 May 87 13:42:19 PDT

Excerpt of an article I posted to RISKS:
>A few days ago on our university UNIX system (4.3BSD), a friend of mine
>received the message reprinted below. Very briefly, someone seems to
>have cracked the passwords in the "passwd" file ...
PGN's reply:
> [I thought using the SALT offset was standard by now! Ho hum,
> another lesson ignored. So, we run it ONE MORE TIME here. PGN]

Bad news, I'm afraid: we _do_ use the salt offset. That's one reason I thought the incident interesting enough to post.

Password attacks (RISKS-4.83)

<Jerome H. Saltzer <Saltzer@ATHENA.MIT.EDU<>
Tue, 12 May 87 10:46:45 EDT

Unless I missed something, the SALT offset doesn't help against the attack this guy was hit with. It just slows things down, but not enough to make it infeasible. The attack consists of taking a copy of the system's one-way password encrypting program, and a dictionary, list of popular first names, list of names of rock groups, or whatever, and encrypting every string in the list, using the SALT of the first user. Then you do it again for the second user. Etc. Depending on the consciousness level of the installation, you typically discover anywhere from 10% to 90% of the passwords that way. We run the program on our staff occasionally, just to keep them on their toes.

These days, if you have a MicroVAX II available -- or a VAX 8600 -- and one of the better DES implementations, you can check out an astonishing number of BSD UNIX possibilities overnight.
Jerry

[The problem is that the SALT for each user is implicitly available to the attacker, so that individualized attacks are still possible -- although the system-wide dictionary attack is no longer available. The conclusion is that this approach is not really worth its SALT. For those of you new to this one, dig up the paper "UNIX Password Security: A Case History", by Bob Morris and Ken Thompson, CACM, November 1979, vol 22, no 11, pp. 594-597. PGN]

Re: password cracking

Dave Curry <davy@ee.ecn.purdue.edu>
Tue, 12 May 87 08:18:27 EST

Before this starts a flurry of speculation about whether or not the UNIX password encryption is secure or not... I seriously doubt that this person has actually *cracked* the algorithm. If you examine the code, you will see how truly difficult that would be, since much of the information you need is discarded and not present in the encrypted result.

> As an experiment, and something of an unofficial public service, I
> have been experimenting with a password breaking program that was
> recently released into the public domain...

This sounds very much like a program I wrote a few years ago to check for "stupid" passwords on our machines. My program simply made some educated guesses on passwords - first name forwards, backwards, capitalized, not capitalized... last name the same way... login name the same way. In all a total of 12 guesses per account. In one night's processing time on our Gould PN9080, I got about 480/10,000 a real word. [...]

--Dave Curry

Re: Computer thefts (Jerome H. Saltzer, RISKS-4.83)

Michael Wagner +49 228 303 245 <WAGNER%DBNGMD21.BITNET@wiscvm.wisc.edu>
Tue, 12 May 87 18:21 CET

At University of Toronto, where I used to work, we convinced our terminal vendor to supply us with special terminals for public terminal clusters. These terminals had bolts, built into the base, that were intended to bolt through the terminal table. Once attached, the bolts could not be removed with standard tools. Neither could the terminal be opened to remove the bolts that way. It helped, although I gather there were still some terminals that walked away. I think that, at least in some cases, the table went too. After all, it was a nice terminal table!

Michael

Computer-related Cadillac recall (RISKS-4.81)

Jeffrey R Kell <JEFF%UTCVM.BITNET@wiscvm.wisc.edu>
Tue, 12 May 87 10:41:05 EDT

This incident (and many others) represents one excellent reason why some systems are best left 'low-tech'. Headlights can burn out, electrical systems fail, batteries die, alternators short, switches malfunction, and so forth. Adding a computer into the chain only adds another item which can possibly fail WITHOUT providing any greater reliability in the process; in perfect working order it is STILL prone to previous faults PLUS the possibility of hardware/software/RFI/etc. failures.

Search RISKS using swish-e

Report problems with the web pages to the maintainer

Search RISKS using swish-e

THE RISKS DIGEST

Forum on Risks to the Public in Computers and Related Systems

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

Volume 4: Issue 85

Thursday, 14 May 1987

Contents

Holiday reading

Jim Horning <horning@src.DEC.COM>
Wed, 13 May 87 17:38:03 PDT

During my recent vacation in Washington, DC, I got a chance to look at a couple of documents that I haven't seen discussed in RISKS:

1) APS PHYSICS AND SOCIETY, vol. 16, no. 2, April 1987, pp. 8-9:
"SDI Software: The Telephone Analogy. Part II: The Software Will Not Be Reliable," K. Dahlke, et al.

This is a piece co-signed by 16 members of the Bell Labs staff.

> On December 3, 1985, Sol Buchsbaum, executive vice president of AT&T Bell Laboratories, testified before the Senate Subcommittee on Strategic and Theater Nuclear Forces. In his statement, Dr. Buchsbaum compared the Strategic Defense Initiative (SDI) to the United States telephone network, in order to demonstrate the technical viability of

> SDI. We feel this comparison is irreparably flawed. ... Many of us
> design the very telecommunications systems Dr. Buchsbaum references.

The same issue reprints Buchsbaum's testimony and has two articles on inexpensive countermeasures to space-based weapons systems.

2) "Report to The American Physical Society of the Study Group on Science and Technology of DIRECTED ENERGY WEAPONS," April 1987, to be published in REVIEWS OF MODERN PHYSICS. 400+ pp.

> The APS convened this Study Group to evaluate the status of the science
> and technology of directed energy weapons (DEW). ... This action by
> the APS was motivated by the divergence of views within the scientific
> community in the wake of President Reagan's speech on March 23, 1983
> in which he called on the U.S. scientific community to develop a system
> that ``... could intercept and destroy strategic ballistic missiles
> before they reach our soil...''.
>
> The APS charged the Study Group to produce an unclassified report,
> which would provide the membership of the Society, other scientists
> and engineers, as well as a wider interested audience, with basic
> technological information about DEW.*

The study group consisted of 17 blue-ribbon physicists chaired by N. Bloembergen of Harvard University. The review committee consisted of G. Pake, M. May, W. K. Panofsky, A. Schawlow, C. Townes, and H. York. Their principal finding is that

> Although substantial progress has been made in many technologies
> of DEW over the last two decades, the Study Group finds significant
> gaps in the scientific and engineering understanding of many issues
> associated with the development of these technologies. Successful
> resolution of these issues is critical for the extrapolation to
> performance levels that would be required in an effective ballistic
> missile defense system. At present, there is insufficient information
> to decide whether the required extrapolations can or cannot be
> achieved. Most crucial elements required for a DEW system need
> improvements of several orders of magnitude. Because the elements
> are inter-related, the improvements must be achieved in a mutually
> consistent manner. We estimate that even in the best of circumstances,
> a decade or more of intesive research would be required to provide
> the technical knowledge needed for an informed decision about the
> potential effectiveness and survivability of directed energy weapon
> systems. In addition, the important issues of overall system
> integration and effectiveness depend critically upon
> infomation, that, to our knowledge, does not yet exist.

They go on to say that

> We estimate that all existing candidates for directed energy weapons
> require two or more orders of magnitude (powers of 10) improvments in
> power output and beam quality before they may be seriously considered
> for application in ballistic missile defense systems. In addition,
> many supporting technologies such as space power, beam control

and delivery, sensing, tracking, and discrimination need similar improvements over current performance levels before DEWs could be considered for use against ballistic missiles.

The part most relevant to RISKS is Appendix A: Issues in Systems Integration, which raises issues frequently mentioned on RISKS, e.g.

Decentralization may increase the problems of command and control, while more centralized organization may entail increased vulnerability.

* A personal footnote: I think that ACM has failed in its obligations to its members and to society by not chartering an analogous study of the computing technology needed for ballistic missile defense. It's very late to start one now, but perhaps this is a case of ``better late than never?''

Jim H.

Hey, buddy, wanna buy a phone call cheap?

Peter Neumann <Neumann@CSL.SRI.COM>
Wed 13 May 87 19:02:24-PDT

Source: "New Breed of Hustler: Selling Illicit Long-Distance Phone Calls", by Robert D. McFadden, New York Times, 11 May 87.

A new multimillion-dollar scam is underway in this country. Hustlers at bus and rail terminals and other convenient places all over the U.S. are selling unlimited-length long-distance telephone calls at a discount. The going rate at the New York's Port Authority Bus Terminal is $2 for calls anywhere in the country, and maybe $4 for international calls. The entrepeneur places your call with a calling code from telephone company computers and distributed like drugs through various networks, human and/or electronic. The ``stealing'' of codes is apparently quite widespread.

There were 190 arrests in New York last year. $500 million is the current estimate of illegal calls per year. With AT&T, MCI, Sprint, and others all using just a sequence of digits for identification, this can be expected to grow. (Perhaps British Telecom's PhoneCard is the right idea, if it can be made mostly fraud-proof.)

Re: Information Age Commission

<TMPLee@DOCKMASTER.ARPA>
Wed, 13 May 87 03:03 EDT

In 4.84 Wm Brown III seems to have inferred (and implied) that my comment about the propriety (or expectations) of sharing RISKS with Congress said something about my views on the proposed legislation. Not true: I'm constantly torn between the view that Congress (as well as the press) knows nothing about any quasi-technical issue and the view

that they are about the only institution we have to save us from ourselves; in this case I haven't formed an opinion (not that it would matter much to anyone.)

Information Age Commission (RISKS-4.84)

<ptsfa!pbhya!seg@Sun.COM>
Wed, 13 May 87 16:29:30 PDT

> There are some potentially useful things government *could* do for us, ...
> The only body which can realistically offer protection against such abuses
> is a more powerful government agency, such as Congress.

No chain is stronger than its weakest link. Because far too many senators and congressmen lead lives that they wish to keep private, such as Gary Hart, powerful investigative agencies, such as the FBI under J. Edgar Hoover, were able to control important congressional leaders.

SEG

[This note is marginally relevant. But insofar as the role of governmental leaders is vital to the proposed Commission, it is included here. No debate please. Just recognition that we are all human. PGN]

Information Age Commission and the number of readers of RISKS

David Sherman <mnetor!lsuc!dave@seismo.CSS.GOV>
Thu, 14 May 87 08:25:11 EDT

>From: Richard A. Cowan <COWAN@XX.LCS.MIT.EDU> Re: RISKS DIGEST 4.84
>
>Given that the RISKS digest is distributed to hundreds, or even thousands ...

People on the ARPAnet side may not realize how extensive that distribution is. RISKS is gatewayed to a Usenet newsgroup (formerly mod.risks, now comp.risks). Brian Reid's monthly newsgroup statistics estimate for as of April 1987 there were 7,100 people who actually read RISKS on the Usenet side alone.

As to whether RISKS is a public forum, the same statistics estimate that 859,000 people have access to Usenet, and 180,000 of those actually read netnews. You can draw your own conclusions.

David Sherman, The Law Society of Upper Canada, Toronto
{ seismo!mnetor cbosgd!utgpu watmath decvax!utcsri ihnp4!utzoo } !lsuc!dave

---

Lockable computers

PAT <HAYES@SPAR-20.ARPA>
Wed 13 May 87 11:04:13-PDT

Your correspondence about the need for a physical lock on students motherboards was recirculated on INFO-COBOL, presumably as part of the uproarous laughter. This is just to say how much I agree that some such feature is necessary, and to add to your sadness that such mundane matters as the circumstances of real life are not taken seriously by designers. Tell them to go look at how televisions are often modified by visual-aids resource centres in colleges. Pat Hayes

---

How a Computer Hacker Raided the Customs Service -- Abstrisks (a nit)

<Paul F Cudney <Cudney@DOCKMASTER.ARPA<>
Wed, 13 May 87 01:51 EDT

(Re: Risks 4.83)

I am confused. Why would Customs propose to provide $8M to the Coast Guard when they had already "donated" their two planes? Somehow the actions of the Coast Guard would be more believable if Customs had received the planes.

Is this an abstract risk? Paul

[Relations were bad after the planes were reassigned from Customs to CG. During a subsequent thaw in the bad relations that ensued, Customs promised CG $8M to help the CG's airborne drug interdiction program. DeConcini said don't do it. CG took the money out of Customs' narcotics traffickers operating account.

Sorry. I should have been more explicitive-deleted. PGN]

Search RISKS using swish-e

THE RISKS DIGEST

Forum on Risks to the Public in Computers and Related Systems

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

Volume 4: Issue 86

Monday, 18 May 1987

Contents

ATM Fraud

<Chuck.Weinstock@sei.cmu.edu>
18 May 1987 10:59-EDT

The Wall Street Journal (18 May 87) has a Page-One article about one Robert Post, a 35 year old former ATM repairman who has beaten New York City ATM's out of $86,000. He'd spy over customer's shoulders to get their PIN, and if they left the receipt he'd take it to get their account number. Then he'd go home and forge a card using a $1,800 machine he bought, and return to the ATM and make withdrawals.

He was caught because his encoding of the account number and the PIN, while good enough to work in the machine, was flawed. Manufacturers Hanover managed to program its network to detect the flawed cards and capture them. After capturing two and verifying that they were fake, they reprogrammed the machine to notify security when one was being used, and dispatched guards to catch Mr. Post.

Mr. Post, who repaid $50,000 to Manufacturers Hanover, had expected to get

off with a hand slap. So far that hasn't happened. He contrasts himself favorably with someone who mugs a customer and steals the card. "I'm a white collar criminal." He was dismayed that bank officials didn't offer him a consulting job.

Chuck

Between Iraq and a Hard Place [Protect Your Phalanx]

William D. Ricker <wdr%faron@mitre-bedford.ARPA>
Mon, 18 May 87 13:20:48 edt

Today's Wall Street Journal (5/18/87) has this front-page item:

US Guided Missile Frigate hit by Iraqi missile, probably Exocet, in Gulf.

[Hearsay report from CBS Newsradio says the Phalanx close-in defense gun, which the Boston Globe reports the class carries, is (for safety reasons) turned on only when in free-fire zones--i.e., the fully-automatic computer controlled weapon is not considered safe enough to tell when the ship is under surprise attack (probably a good idea), but isn't used to inform the crew when it needs to be enabled..]

--Bill Ricker

<minow%thundr.DEC@src.DEC.COM>
Sat, 16 May 87 15:39:58 PDT

(Martin Minow THUNDR::MINOW ML3-5/U26 223-9922 16-May-1987 1831)
To: "risks@csl.sri.com"@src.DEC.COM
Subject: Wozniak Scholarship for Hackers

From the Boston Globe, May 16, 1987:

> Boulder, Colo. - Computer whiz Stephen Wozniak has donated $100,000 for a University of Colorado scholarship aimed at developing excellence in computer hackers at his alma mater. "The value of cracking security codes and understanding them is that it generates incredible knowledge," said Wozniak, one of the original hackers and co-founder of Apple Computer Inc. Wozniak said he actually encourages the "mildly social deviants" to break access and security codes as a way to learn, The Denver Post reported. The "Woz" scholarship program is two-fold; a tuition grant and a job working with the computer science department.

Martin Minow

P.S. One of the beauties of the English language is that you don't know whether Wozniak is encouraging (mildly (social deviants)) or ((mildly social) deviants).

[I was struck by "incredible knowledge." Woz probably did not mean "knowledge of the incredible", but if the knowledge is incredible, there is the nice ambiguity between "so extraordinary as to seem impossible" (particularly if true) and "unbelievable" (particularly if NOT true). PGN]

Information Overload and Technology?

David Chess <CHESS@ibm.com>
14 May 1987, 12:37:07 EDT

Long Ago (Risks 4:66), Dave Taylor wrote
> Overcoming Information Overload with Technology (Why It Can't Work)
> I'm especially interested in horror stories people could tell me about
> relying on information filtering systems and finding that they actually
> weeded out critical information...

This strikes me as not quite the right tack to be taking (although I haven't read the full paper). Certainly it's worthwhile to gather "horror stories", for the purpose of improving information filters, and making people aware of their limitations, but it doesn't seem valid to conclude that "It Can't Work".

Everyone uses some information filter; this is pretty much tautological, since there is much more information available in the world than anyone not otherwise idle can possibly keep up with. So we limit our intake with techniques like

- Choosing to ignore broad classes of information ("I don't have time to follow AI-list anymore" "Please drop me from...")
- Never reading any article whose title doesn't immediately "grab the eye"
- >Haphazard< filtering, caused by just reading whatever one happens to have time to read. This month I get around to reading RISKS, but don't have time for NL-KR. Maybe next month if NL-KR shows up first, it'll be vice-versa.

Now all these filtering techniques (especially the last!) have in common a relatively large risk of missing important stuff. None of them is very sophisticated, or very likely to work very well. I would be *quite* surprised if it turned out that computers (much less "technology") could not make the process work better. Certainly there will be horror stories about the use of the technology, but (if we had a way to collect them), I suspect there'd be even more about filtering *without* the technology...

This is the usual sort of meta-risk. Certainly using computers to do X won't work all the time, and we'll be exposed to risks; but doing X without the computers is at least as risky!

Dave Chess, Watson Research Center

(Any opinions that might have snuck in here are my own, and are not necessarily shared by my employer)

Passwords, thefts

Andrew Burt <isis!aburt@seismo.CSS.GOV>
18 May 87 20:58:10 GMT

The real attacks to be worried about are not password attacks. As administrator of the Unix security mailing list I see all the latest holes (three easy steps to root, etc.). Some of the holes are truly frightening. Once a hacker has access to a system (as guest, whatever) he need not spend much time trying to work out someone else's password -- might as well go straight to root.

System administrators are also welcome to join the USML; to cut down the number of invalid requests to join I ask that you send mail to me as root; further validation is done after that. (I apologize for the amount of red-tape but the explicit nature of the information discussed demands some protection.)

> [Since it is so easy to dig the root, I wonder how many bogus requests you will get! Like a pig rooting for troubles? PGN]

>From: Michael Wagner <WAGNER%DBNGMD21.BITNET@wiscvm.wisc.edu>
>Subject: Re: Computer thefts (Jerome H. Saltzer, RISKS-4.83)
>... These terminals had bolts, built into the base, ...

Here at DU we have the terminals bolted to long conference tables -- rather hard to walk out with. Far better, though, is that each unit is engraved and painted with large "DU"s on each component in highly visible locations. Makes them very hard to fence. (Sure, you can use the innards, but then again you could engrave the boards...)

I haven't heard of any terminals or PC's walking out since this was done.

Andrew Burt isis!aburt

passwords, sexual preference and statistical coincidence?

Robert W. Baldwin <BALDWIN@XX.LCS.MIT.EDU>
Wed 13 May 87 07:17:55-EDT

I've been working part time on a case study of password usage on MIT's undergraduate machines. The fast password transform that is currently available was developed by myself and improved with the help of several people at other research centers. It turns out that the SALTing that prevents the use of DES chips can be implemented by five instructions in each round of the DES F function.

The case study should be available by the end of the summer, but I would like to point out one risk that arises when a person chooses a first name for a password. This is an example of the principle of guilt-by-statistical-coincidence.

I tried a dictionary of 2000 first names against all 4100 accounts. The program uncovered the passwords for seven percent of

the accounts. This took 6 hours on a VAX/8600 and it was helped by the fact that the 4100 accounts only use 1735 different SALT values.

Moving into the domain of sociology, I examined whether people chose names of the same or opposite sex. I found that 80% of the users chose passwords of the opposite sex. An additional 7% chose a variant of their own first names. The remaining 13% had picked names of the same sex.

The coincidence is that the student group, Gays At MIT, claims that 10-15% of the undergraduates are homosexual. The conclusion one could draw is that anyone with a same-sex password is either narcissic or gay. Anyone who uses an opposite-sex password is heterosexual, and if it is not the name of their current significant other they are having an affair. Send the police if they pick their mother's or father's name. Perhaps this could persuade people not to use names as passwords.

--Bob

[This message has some interesting background on risks of passwords, but the statistical conclusions are almost as accurate as this:

About 25% of all people are males living in the East.
About 25% of all people are females living in the West. Therefore,
most males living in the East are females living in the West.

But not quite.

At any rate, I hope the message is getting through that passwords can be relatively easy to break. For a REALLY BEAUTIFUL DESCRIPTION of a horrendous implementation flaw in a well-known system (which is not named), see an article by Bill Young and John McHugh (Coding for a Believable Specification to Implementation Mapping), on pp. 141-142 of the Proceedings of the IEEE Symposium on Security and Privacy, April 1987. The bug has presumably been fixed everywhere by now, but it permitted an easily constructed overly long password to fake out the encrypt-and-compare algorithm. I have known about this one for years, and am delighted to finally see it in print. PLEASE dig up this article. It is well worth reading. PGN]

Search RISKS using swish-e

Report problems with the web pages to the maintainer

Search RISKS using swish-e

THE RISKS DIGEST

Forum on Risks to the Public in Computers and Related Systems

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

Volume 4: Issue 87

Wednesday, 20 May 1987

Contents

Computer Libel: A New Legal Battlefield

Peter G. Neumann <Neumann@CSL.SRI.COM>
Tue 19 May 87 17:32:02-PDT

DIGITAL REVIEW, 18 May 1987, p. 72 [although the page is unnumbered]

> ... databases inherently carry a high risk of error. Information can be altered or partially deleted through inadvertent mistakes or deliberate manipulation. Abstracts of data can be misinterpreted, especially when taken out of context. Failuer to update a database periodicaly can result in the dissemination of incorrect information about a company or an individual. And hardware and software malfunctions can compound all these problems.
>
> Here are a few examples of the havoc an erroneous computer search can cause:

* A computer analysis of several thousand New York welfare recipients found that more than 20 percent were working. On the surface, this seemed like a violation of state law. But a second check disclosed that more than half of those individuals had been authorized to work while receiving welfare benefits. Apparently their files had not been updated.

* A Dallas executive traveling on business in New Orleans was stopped by police for a minor traffic infraction. When the computer wrongly flagged him as an escaped convict, he was arrested and jailed. It took a week to correct the error.

* A New York electronics manufacturer, ready to close on a $2 million contract, was taken aback when the banks refused to give him the needed loans. It turned out that a financial check had mistakenly shown his company to be bankrupt.

The article discusses the Supreme Court ruling on Dun & Bradstreet vs. Greenmoss Builders, in which D&B had falsely reported that GB was broke. The Supreme Court upheld the Vermont decision against D&B. The article goes on to consider some other legal issues.

This means that information vendors can no longer use the following rationales to wriggle out of paying for their errors:

Free speech umbrella. Although data vendors have a First Amendment right to free speech, they also have an obligation to ensure that the information they research and disseminate is accurate.

Public interest argument. The courts have long acknowledged that everyone has a right to comment on matters of public concern. But they also have noted that information on the private finances of companies and individuals, unless they seek the limelight, is not of public interest.

"Chilling effect" standard. The need for a free exchange of ideas demands that we occasionally tolerate the foibles of the press, as long as there is no malice. The media have argued that to do otherwise would have a "chilling effect" on reporting. The courts, however, have not extended this argument to data vendors.

Public domain argument. It is quite well known that government agencies engage in periodic fishing expeditions, matching data and peeking through giant data banks to ferret out criminal activity. But private data vendors don't have the government's license to snoop. In fact, they must comply with state and federal privacy laws when conducting such searches, and if they err, they are accountable.

Electric chair tested by car insurer

<bfisher.ES@Xerox.COM>
20 May 87 15:17:18 PDT (Wednesday)

This is from the Design International column of MACHINE DESIGN of 3/26.

An electric chair designed to help prevent car theft has been teamed with an electronic alarm and tested by a leading Swedish insurance company, Skandia of Stockholm. Built-in electric cables are activated after the alarm has sounded four times. The shock transmitted to the person in the driver's seat is about 9kV at an inductive current of 65uA. Although unpleasant, the shock is not harmful even to people suffering from heart ailments, according to the company.

(Clockwork Orange is alive and well??!!)
Bill Fisher

Computers and Open Meetings laws

Barbara Zanzig <barbaraz%hawkeye.gwd.tek.com@RELAY.CS.NET>
Wed, 20 May 87 11:03:39 PDT

I've never seen anything like this appear in either Risks or comp.society, so I'm sending this along to both.

An editorial in The (Portland) Oregonian:

OPENNESS RESISTS CHIPPING

Oregon is inching toward truly interactive local government. The Gresham City Council has voted to supply its members with computer terminals in their homes, to enable them to do research in the city's system at any time.

Providing unpaid elected officials with the tools to do their job better is easily worth the $6,000 appropriated for this purpose. But in a state with a strong Open Meetings Law and Open Records Law, does technology now require an Open Electronic Impulses Law?

The Gresham computer system, like many others, permits users to send messages to other users. Anyone with a modicum of conspiracy theory can easily imagine a quorum of the City Council logged on to their computers together, busily conducting city business beyond the prying eyes of those without user codes.

Gresham officials realize the risks involved. Even if city residents cannot gain access to the system, the information in it still belongs to them. And since a private conference call among a council quorum is illegal, a computer caucus would equally constitute an access violation.

"What goes in is something we're concerned about, and I will probably advise them to be conservative," says City Attorney Tom Sponsler. "For council members to communicate, with a quorum, on how they feel about policy is not appropriate, and I will so advise them."

Sponsler thinks there is a greater potential for violations of the Open Records Law than the Open Meetings Law. "Anything of any substance," he

advises, "should not exist only online." Members should also remember, as Lt. Col. Oliver North could remind them, that anything put into a system can later be pulled out of the system.

City Manager Wally Douthwaite expects that before the system goes on line, Gresham will need a written policy on its use. The need for clarification may not stop there.

"There may be a time when computer use will be so universal that we will need to take another look at the law," says Oregon Attorney General Dave Frohnmayer. "The Open Meetings Law was not designed for this technology."

The rules, Frohnmayer and Sponsler agree, should be clear. Providing information by computer is fine; debating and negotiating electronically slips into silicon secrecy.

If the legal principle is clear, the technology should be able to follow. All that is needed by Gresham - and the cities that will doubtless follow its example - is a package of Open Meeting Software.

And people who understand its importance.

***[end of editorial]

I spoke to the reporter who covered the story, and he said it was an email system, not an interactive conferencing system. He thought they'd be using a VAX 220 (?), and didn't know which operating system.

Barbara Zanzig
{major backbone sites}!tektronix!tekecs!barbaraz
barbaraz@tekecs.tek.com

Re: Phalanx

<Chuck.Weinstock@sei.cmu.edu>
19 May 1987 09:18-EDT

If the defense weapons were not reliable enough to keep on all of the time, that should tell us all a lot about the chances for Star Wars to succeed (as if we didn't know already!)

> [There is a serious lesson about perpetual readiness when nothing ever seems to be happening. Too often there appears to be no urgent need to worry about some particular event, because it has never happened before. Someone on board was quoted as saying exactly that -- no one had ever fired anything directly at them before, and therefore it seemed quite reasonable to expect that this time was no different. Crying "wolf" is bad, but not recognizing the wolf (in sheik's clothing?) is even worse.) Sorry if I repeat myself on this subject, but this is a really important issue. PGN]

Choosing a password

<bowen%sevax.prg.oxford.ac.uk@Cs.Ucl.AC.UK>
Tue, 19 May 87 11:20:08 BST

Following the recent discussion on password (in)security, here is a simple way of choosing a fairly safe password which I believe is attributable to Steve Bourne (ex Bell Labs). Find any handy document (there's usually something near most VDUs) and point your finger randomly at the text. Select the nearest word (or words if they are short) and substitute one or two of the letters for some other character. E.g. a `0' for an `o'. This should reduce the risk of your password being decrypted. You also have the benefit that you can easily select a new password as often as you like.

Jonathan Bowen, Oxford University Computing Laboratory, England.

> [Because this is not a deterministic algorithm, it has some merit. However, you must remember that passwords are still vulnerable to various attacks. In some operating systems and in most local networks, it is easy to capture a password in transit. In that case, it does not much matter how cute you are in generating passwords. A second point is that as soon as you let people generate their own passwords, someone will want a nice simple easily guessable one, ignoring the problem that his/her operating system does not do a very good job of preventing someone masquerading as that user from climbing through other people's files, implanting Trojan horses, deleting files, etc. It is very antisocial of anyone to have such a weak password, or to rely on passwords that can be easily captured. Simplistic thinking is the real source of trouble. Even the policy that everything should be wide open (no secrets) does not protect you against getting clobbered by file deletions and Trojan horses.
>
> So, let's avoid fine-tuning essentially weak approaches and remember the big picture. Then I will stop reiterating... PGN]

<Michael Wagner +49 228 303 245>
Wed, 20 May 87 14:03 CET

<WAGNER%DBNGMD21.BITNET@wiscvm.wisc.edu>
Subject: Re: Passwords, thefts (Andrew Burt) (RISKS DIGEST 4.86)
CC: isis!aburt@seismo.css.gov

> Here at DU we have the terminals bolted to ... tables ... .
> Far better, though, is that each unit is engraved and painted
> with large "DU"s on each component in highly visible locations.
> Makes them very hard to fence.

Interesting ... we seem to be concerned with different risks. I always assumed that terminals were stolen from public terminal areas in universities by individuals who wanted a home terminal. It never occured to me that someone would seriously consider 'fencing' such a thing. PCs,

perhaps. I guess the general population might know what to do with such things. But terminals?

Under my set of assumptions, a large logo would merely enhance the value of the treasure. In fact, at UofT, we lost a few terminals to start-of-year initiation rights. One terminal made it's way to another university in the area as part of a scavenger hunt (I expect they got extra points for distance).

Does anyone have any statistics on where the real risks are here?

Michael

Nuclear Plant Emergency Plan: In Event of Quake, Smash Toilets

<Don Hopkins <don@brillig.umd.edu<>
Sat, 16 May 87 18:36:46 EDT

Nuclear Plant Emergency Plan: In Event of Quake, Smash Toilets
United Press International

CHATTANOOGA, Tenn., May 14 -- Among the earthquake emergency plans at the TVA's Sequoyah Nuclear Plant is one to break all the toilets with a sledgehammer and cover the plumbing holes with duct tape to seal off nuclear leaks. According to The Chattanooga Times, TVA nuclear engineers decided in 1984 that an earthquake could cause water in toilets to spill or drain out, destroying the "water seal" in the pipes.

At the Watts Bar Nuclear Plant, being built near Spring City, Tenn., plumbing that would not rely on a water seal was installed. But at the Sequoyah Nuclear Plant, where nuclear reactors were operating at the time, the hammer-and-duct-tape plan was adopted. Both reactors at Sequoyah have been shut down for 21 months because of safety and other regulatory violations at the Soddy-Daisy plant. The hammer and tape are stored in a locked wooden box outside the Sequoyah control room.

"Personally, I don't think the big hammer is a big issue," Sequoyah shift engineer Jeffrey Lewis said. "That cabinet has been there for years and we haven't used an inch of duct tape." Clerk Sue Hartman works near the box where the hammer is stored. She said the key to the box is "kept under surveillance at all times." In fact, the key to the key to the cabinet where the hammer box key is stored is "kept on my body," Hartman said.

Search RISKS using swish-e

THE RISKS DIGEST

Forum on Risks to the Public in Computers and Related Systems

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

Volume 4: Issue 88

Thursday, 21 May 1987

Contents

Re: Phalanx

Phil Ngai <amdcad!phil@decwrl.DEC.COM>
Thu, 21 May 87 09:53:45 PDT

The Phalanx is just a radar controlled machine gun which fires 3000
(20 mm? nearly one inch in diameter) depleted uranium slugs per minute
at anything which moves. Would you keep it on all the time? No one
(but you) said it wasn't reliable.

What does appear to be wrong is that there was only one, to cover the
stern of the ship. The bow was not protected by a Phalanx system and
that is where the (two?) Exocet missiles hit.

Then again, we should realize that frigates such as this one are intended
mostly for anti-submarine/mine work; although it did have surface to air
missiles which could have been used to take out the aircraft which fired the
Exocets, frigates are not really expected to provide their own air defense.
And this one was operating under the assumption that Iraq aircraft were
friendly, so it did not shoot down the aircraft when it could have.

[Perhaps the object was to shoot down the missiles? Was that the Star Wars analogy to which Chuck was referring? Also, there was a report that there might have been TWO planes. (One missile landed undetonated amidship!) PGN]

Open meeting laws (RISKS 4.87)

<parnas%QUCIS.BITNET@wiscvm.wisc.edu>
Thu, 21 May 87 07:12:23 EDT

Do open meeting laws prevent public representatives from conversing in a bar or a park or at a theatre? Do they prevent telephone calls? If not, why should they prevent electronic mail conversations?

Dave

[Even my home town of Palo Alto is going through the pains of trying to make sense of the legal and common-sense implications... PGN]

Concerning UN*X (in)security

Mike Carlton <carlton@ji.Berkeley.EDU>
Thu, 21 May 87 13:41:45 PDT

I think that most people would agree that UN*X is not a secure system, nor is it intended to be. However, a judicious choice of password can discourage amateur or half-hearted attacks on your account. Several methods have been proposed for choosing hard to break passwords; my favorite is simply to use the first letter of each word of some phrase, e.g., 'The rain in Spain falls mainly in the plain' becomes TriSfmitp. This has the advantages that it is not likely to appear in any dictionary, it is very mnemonic and if the password is long enough and rich enough in case, it will stand up to a sustained exhaustive search.

There is another risk that I haven't seen mentioned: the use of .rhosts files (at least it's a risk in the BSD world, I've never been in the System V world). Around here, quite a few people have .rhosts entries for several machines, often including at least one Sun. Couple this with the fact that, given physical access, anyone can become root on a Sun and you've got widespread vulnerability without the need for any password attack.

Mike Carlton (carlton@ji.Berkeley.EDU), CS Gradual student

Ed Joyce, Software Bugs: A Matter of Life and Liability

Eugene Miya <eugene@ames-pioneer.arpa>
Thu, 21 May 87 13:47:06 pdt

Ed Joyce, Software Bugs: A Matter of Life and Liability, Datamation 33 10,

15 May 1987, pp. 88-92 [Keywords: Malfunction 54, Therac 25, dosimetry, radiation therapy].

--eugene miya

Risks and system pre-login banners

Peter G. Neumann <Neumann@CSL.SRI.COM>
Thu 21 May 87 20:19:10-PDT

RISKS recently ran an item about the lawsuit that was thrown out because a user had been greeted with "Welcome to the system". The following banner is given by a net-accessible system (which might as well remain nameless), and provides a nice example of the other end of the spectrum.

WARNING ** WARNING ** WARNING ** WARNING ** WARNING ** WARNING

UNAUTHORIZED ACCESS TO THIS UNITED STATES GOVERNMENT COMPUTER SYSTEM AND OR SOFTWARE IS PROHIBITED BY PUBLIC LAW 98-473. PUNISHMENT FOR OFFENSE CAN BE UP TO $100,000 FINE OR UP TO 20 YEARS IN PRISON OR BOTH. REPORT UNAUTHORIZED USE OR ACCESS TO THE SYSTEM SECURITY OFFICER.

WARNING ** WARNING ** WARNING ** WARNING ** WARNING ** WARNING

Waiting mail (msg.a000284) [Risks of Running RISKS, Cont'd.]

ALMSA-1 Memo Service 750 (MMDF 4/84) <mmdf@ALMSA-1.ARPA>
Thu, 21 May 87 12:31:45 CDT

> [As I have noted previously, in a list as large as RISKS there is an awesome volume of mailer barf messages. I do try to be patient, but sometimes it becomes overbearing. The implied threat here -- to keep retrying and send me notifications -- is horrendous! PGN]

After 14 days (326 hours), your message has not yet been fully delivered. Attempts to deliver the message will continue for 178956963 more days. No further action is required by you.

[********* = !!!!!]

Delivery attempts are still pending for the following address(es):

wmartin@almsa-2 (host: almsa-2) (queue: almsab)

Problems usually are due to service interruptions at the receiving machine. Less often, they are caused by the communication system.

Report problems with the web pages to the maintainer

Search RISKS using swish-e

THE RISKS DIGEST

Forum on Risks to the Public in Computers and Related Systems

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

Volume 4: Issue 89

Sunday, 24 May 1987

Contents

Factory Robots Killing Humans, Japan Reports

Peter G. Neumann <Neumann@CSL.SRI.COM>
Fri 22 May 87 17:18:46-PDT

A series of mysterious deaths in which industrial robots suddenly attacked and killed humans is being investigated in Japan, news reports said yesterday. Ten people have been killed by robots in the last eight years. In four cases, operating errors were blamed. In the other accidents, the robots suddenly started working for unexplained reasons, according to reports. Witnesses listed a number of cases in which the robot suddenly

stretched out its mechanical arms, killing its victim. Experts plan to test a theory that electromagnetic waves in factories have been responsible for setting off the sensitive computer mechanisms in the robots.

SF Chronicle 22 May 87, from Deutsche Presse-Agentur.

> [We had previously documented the 1981 Kawasaki case, and noted reports of at least four more (and possibly as many as 19) robot-related deaths. If we have any readers in the far East who can tell us what is really happening, please ... PGN]

Mysterious BART power outage

Peter G. Neumann <Neumann@CSL.SRI.COM>
Sun 24 May 87 11:24:24-PDT

The San Francisco Bay Area Rapid Transit had an unexplained power failure on 17 May 1987, unprecedented in their 15-year history. 17 switches (which act like breakers and shut off power when a short circuit or overload occurs) kicked open in the rush to get runners to the Bay-to-Breakers race (no pun intended), with still no cause having been identified. A train stalled in a tunnel beneath 7th Street in Oakland, and 150 passengers had to walk for 20 minutes to get out. Engineers were unable to restore power in the computer-controlled system. 5 hours later the switches suddenly closed again, just as mysteriously as they had opened.

More on the Master Password attack

Peter G. Neumann <Neumann@CSL.SRI.COM>
Fri 22 May 87 09:56:13-PDT

I received a message questioning my apparent coyness in not divulging the name of a system that had a reported serious flaw. In general I always try to opt for openness, except when I am explicitly not at liberty to divulge something. In the case of the master password bug, it was found long ago in UNIX Version 6 by some colleagues who never disclosed it. The published version that just appeared, and to which I referred, chose not to associate the name of the system with the story. Here are the details.

[Following is my own adaptation of Young and McHugh's presentation, with notation changed to avoid an amazing quadruple overloading of the letter "c"..., and triple overloading of "a" and "b". PGN]

"Constructive" Password Attack: Master-password-generation algorithm
= =
Young and McHugh (Coding for a Believable Specification to Implementation Mapping), pp. 141-142, Proc. IEEE Symp. Security and Privacy, April 1987.

Data structure
= = = = = = = = = = = = = = =
a. User login name

b. User typed password
c. Stored encrypted password
d. Encrypted typed password

The Password Checking Algorithm
= = = = = = = = = = = = = = = = =
1. User typed login name --> a.
2. Stored encrypted PW --> c.
3. User typed password --> b.
4. Encrypt user typed PW --> d.
5. Compare c and d.

Step 1. 3. 2. 4.

Login Name	Typed PW	Stored Encryp	Encryp Typed PW
a	b	c	d

Step 5 compares c and d.

The Master Password Attack
= = = = = = = = = = = = = = = = =
Choose any string, "rst"
Encrypt it, obtaining "xyz"
Enter ANY legitimate user name.
Type password "rstxyz"

The Password Algorithm Overwhelmed

	a	b	c	d
1.	Name			
2.	Name		uvw	
3.	Name	rst	xyz	
4.	Name	rst	xyz	xyz

5. xyz=xyz

The design was more or less sound sound (apart from the intrinsic password problems that we have been discussing in RISKS). However, the implementation was seriously flawed by the absence of bounds checking. Thanks to Young and McHugh for publishing this one.

Measures, countermeasures, and under-the-counter-measures

Peter G. Neumann <Neumann@CSL.SRI.COM>
Sat 23 May 87 11:50:31-PDT

On page 9 of the SF Chron, 23 May 87, there is a small item on the Speaker of the Iranian Parliament. He claimed that the Iranians electronically countermanded the missiles (an Exocet [which did not explode] and the other still unidentified missile, possibly an AS-30 laser-guided missile) AWAY FROM one of their tankers. If that is true, would the Iraqis have realized what happened? (Were any countermeasure devices included in the arms sales to the Iranis?)

Reports persist (with an official denial) that computer systems on the Stark had not been working, and that they were waiting for spare parts. Investigation continues.

Phalanx (RISKS 4.88)

Scott Dorsey <kludge@gitpyr>
Fri, 22 May 87 13:07:50 edt

>What does appear to be wrong is that there was only one, to cover the
>stern of the ship. The bow was not protected by a Phalanx system and
>that is where the (two?) Exocet missiles hit.

The standard configuration on guided missile carriers (I regret to say that I have not seen a frigate with the things yet), is to have one port, one starboard, about 2/3 of the way from the stern. This way, the bow is well protected. The Phalanx is a very short-range system, which is to be used only if everything else fails and the long-range defenses are penetrated. The system was not designed to be rapidly armed. It is expected that the long-range defenses will be able to hold off fire until the Phalanx is available.

>... frigates are not really expected to provide their own air defense.
>And this one was operating under the assumption that Iraq aircraft were
>friendly, so it did not shoot down the aircraft when it could have.

If you shoot at friendly aircraft, they will cease to be friendly. If you don't shoot them, you have to trust them. And sometimes trust is not always justified. The risks involved here are not if you can trust your own systems, but if you can trust your allies' systems.

Scott Dorsey Kaptain_Kludge
ICS Programming Lab (Where old terminals go to die), Rich 110,
Georgia Institute of Technology, Box 36681, Atlanta, Georgia 30332
...!{akgua,allegra,amd,hplabs,ihnp4,seismo,ut-ngp}!gatech!gitpyr!kludge

[Once again, you can't shoot down everything that flies near you. But you can try to shoot down missiles. One report in this morning's paper noted that the Phalanx gets aout 8 out of 10... PGN]

Re: Phalanx

<decvax!utzoo!henry@ucbvax.Berkeley.EDU>
Sat, 23 May 87 22:18:25 edt

> If the defense weapons were not reliable enough to keep on all of the time...

There are actually a couple of issues here. One is the question of wear and tear on continuously-operating mechanical hardware (the Phalanx radar is mechanically scanned, I believe). More significantly, though, *any* such defensive system has some small probability of shooting down a friendly aircraft. Note that this problem is *not* restricted to automated systems! Experienced combat pilots tend to consider "friendly" gunners to be almost as big a threat as "hostile" ones, with good reason. "Own goal" hits are common in real fighting; there were several in the Falklands War, on both sides.

One reason for having different levels of alert is simply to minimize the chances of shooting down the wrong thing at a time when there is little real danger. The problem is particularly touchy when operating in a known war zone with the intent of remaining uninvolved.

Henry Spencer @ U of Toronto Zoology

Computer Bill of Rights

Eugene Miya <eugene@ames-nas.arpa>
Fri, 22 May 87 11:26:20 PDT

I recall 20 years ago (not that I was doing computers then) someone wrote a computer Bill of Rights (for people). Could anyone send me a copy of that? If need be, I will make the document ftp'able on one of our machines here.

--eugene miya, NASA Ames

Credit Information Access

<mcdchg!heiby@seismo.CSS.GOV>
22 May 87 14:51:32 CDT (Fri)

The following appeared on page 48 of the May 18, 1987 issue of Insight magazine. It seems relevant to many issues discussed recently.

Credit Report Access

Car loans, mortgages and credit card applications are approved based on information found in an individual's credit history, but most consumers have never seen their computerized credit profile. Now consumers can get the same easy access to their credit report that banks and other lenders have had for years.

TRW Inc., one of the nation's largest credit reporting agencies with files on some 140 million people, is launching Credentials, the first credit and financial information service sold directly to consumers. For an annual fee of $35, a member gets unlimited access to the credit report supplied to

lenders, notification when any lender reads the file and a credit application that is kept on file and can be electronically sent to lenders with the member's consent.

More than 250,000 became members last year during a pilot program in California. The service is now expanding nationwide.

"Credentials offers consumers greater control over their credit profiles by ensuring their accuracy." says Mel Wellerstein, a vice president at TRW. "Furthermore, with full knowledge of their credit history, consumers are less likely to be taken advantage of or be intimidated by lenders."

Ron Heiby, heiby@mcdchg.UUCP Moderator: comp.newprod & comp.unix
Motorola Microcomputer Division (MCD), Schaumburg, IL

Open meeting laws

<jlh%acorn@oak.lcs.mit.edu>
Fri, 22 May 87 20:01 EST

> From: parnas%QUCIS.BITNET@wiscvm.wisc.edu
> Subject: Open meeting laws (RISKS 4.87)
>
> Do open meeting laws prevent public representatives from conversing in a bar or a park or at a theatre? Do they prevent telephone calls? If not, why should they prevent electronic mail conversations? Dave

I'm the chair of the Cambridge Human Rights Commission, a local agency that is covered by the Massachusetts open meeting law. That law applies to deliberate meetings of a quorum of members for the purpose of taking actions, or discussing actions that the board or commission might take. Any such meetings must be public and announced in advance, minutes must be taken, etc.

With such a law, a phone call or meeting in a bar is okay, so long as there's not a quorum present, or if the meeting was by chance, or serves a social function (rather than the discussion of business).

On the other hand, a computer conferencing system or e-mail, like a conference telephone call or meeting in a bar, is not okay if used for discussions and negotiations among the members of the commission or board, at least not if a quorum of members participate. So the legal advice given by the Gresham City Attorney seems sound to me, assuming the Oregon law is similar to ours.

Roughly speaking, it might be okay to use e-mail or computer conferencing the way you'd use a postal (USPS) mailing list: to send out information unidirectionally. But using it for two-way, back-and-forth interaction is using it as a substitute for a meeting, and that's precisely what's disallowed, because the public doesn't have access. (Even if the computer system were open to the public, you'd be on shaky ground, because most people don't own modems or know how to use e-mail. They'd have as much

"access" as if the meeting were held a thousand miles away.)

From a techno standpoint, that's too bad; computer conferencing has some advantages over meetings (among them, potentially, the existence of a written record). But it's good public policy. As it is, people have difficulty understanding and participating in their government; apathy, bureaucracy, bad public transportation, and the grinding difficulty of 9-to-5 existence are among the culprits. Let's not add computers to the list until we have systems that are truly accessible to lay people from all walks of life.

-Jonathan Handel

PS: I'm not an attorney, so my reasoning is certainly far from definitive. Also, I don't have a copy of the Mass. law in front of me, so this is based on my best recollections. And of course, open meeting laws vary by state, so the issues will vary by state as well.

> [Bruce Baker wondered how I could have avoided making a pun on Gresham's Law in RISKS-4.88. I thought this issue was more like Gresham Slaw, carrying Coles to New Facile. In this case, the bad votes drive out the good? PGN]

Privacy and Email - The Law Takes Notice

<LEICHTER-JERRY@YALE.ARPA>
22 MAY 1987 12:52:33 EST

(Forwarded (ultimately) from a UDEL NEWS bboard.) Jerry

This is a copy of a letter published in MIT Tech Talk. Anyone who did not read that memo should look read it. Be sure to note that operators of electronic communication systems now have legal responsibilities for the privacy of data.

MEMORANDUM

To: The MIT Community
From: James D.Bruce, Vice President for Information Systems
Re: The Electronic Communications Privacy Act

The Electronic Communications Privacy Act of 1986 was enacted by the United States Congress in October of last year to protect the privacy of users of wire and electronic communications.

Legal counsel has advised MIT that its computer network and the files stored on its computers are covered by the law's provisions. Specifically, individuals who access electronic files without appropriate authorization could find themselves subject to criminal penalties under this new law.

At this time, we can only make broad generalizations about the

impact of the Act on MIT's computing environment. Its actual scope will develop as federal actions are brought against individuals who are charged with inappropriate access to electronic mail and other electronic files.

It is clear, however, that under the Act, an individual who, without authorization, accesses an electronic mail queue is liable and may be subject to a fine of $5,000 and up to six months in prison, if charged and convicted. Penalties are higher if the objective is malicious destruction or damage of information, or private gain.

The law also bars unauthorized disclosure of information within an electronic mail system by the provider of the service. This bars MIT (and other providers) from disclosing information from an individual's electronic data files without authorization from the individual.

MIT students and staff should be aware that it is against Institute policy and federal law to access the private files of others without authorization. MIT employees should also note that they are personally liable under the Act if they exceed their authorization to access electronic files.

---

rhosts

Anthony A. Datri <aad#@andrew.cmu.edu>
Fri, 22 May 87 10:33:05 edt

I believe that a year or two ago someone did indeed use rhosts files to cause a lot of trouble at berkeley. Here at CMU we're in the middle of developing a terribly trendy distributed system of sun2/3's, uvaxes, and ibm rt's (ugh). The problems of console access have been causing major headaches, to the point where there now exists an authentication scheme that I admit that I don't understand.

anthony a datri, carnegie-mellon univer$ity

Search RISKS using swish-e

Search RISKS using swish-e

THE RISKS DIGEST

Forum on Risks to the Public in Computers and Related Systems

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

Volume 4: Issue 90

Monday, 25 May 1987

Contents

Laser guided missiles...

<LIN@XX.LCS.MIT.EDU>
Mon, 25 May 1987 13:54 EDT

> From: Peter G. Neumann <Neumann at CSL.SRI.COM>
> ... He claimed that the Iranians electronically countermanded the missiles (an Exocet [which did not explode] and the other still unidentified missile, possibly an AS-30 laser-guided missile) AWAY FROM one of their tankers.

Other messages have also referred to laser-guided missiles. [They] require a laser to designate the target, which the missile then homes in on, by seeking the reflected laser light. That means that there must be a laser actively illuminating the target at all times while the missile is seeking.

If the airplane carrying the missile goes away or drops out of line of sight, it can't illuminate the target.

> [This discussion at the moment is labelled SPECULATION with respect to the Stark investigation in progress. But one question is, how easily can a

missile such as the laser-guided AS-30 be faked out? What happens under cloud cover? Does the missile go inertial for a while if it loses the target, in hopes of reacquiring the target? Can it get confused by decoys, light chaff, fireworks, or whatever? Is the Iranian countermeasure claim plausible? Remember, there were two missiles (the exploded one suspected NOT to be an Exocet?), and if one was electronic and the other laser guided, the countermeasure theory seems less likely. Although I presume analogous arguments hold for electronic countermeasures on electronically guided missiles, the mechanisms might be different... In any case, the risks of hitting something other than the desired target seem to be nontrivial. PGN]

FURTHER RESPONSE FROM HERB:

The AS-30 is indeed a laser guided missile, but it too requires an independent laser designator. If no Iranian airplane or boat was in sight of the ship, no target designation would take place. You must have a line of sight to the target. [Rafsanjani reportedly said that there had been an Iranian tanker in range. PGN]

The AS-30 is described as having two guidance components -- inertial reference for the initial phase, and laser homing for the terminal phase. If anything intervenes between the laser beam and the target, most likely the missile will lock its home-on track, and be lost.

Computer use costs civil servants $1,270 [Canadian Press]

<Matthew_Kruk%UBC.MAILNET@MIT-Multics.ARPA>
Mon, 25 May 87 09:20:40 PDT

OTTAWA - Two federal public servants who used a government computer for their own purposes have been ordered to pay the government $1,270 for misuse of high technology. The environment department billed Michel Grenier and Gaston Boisvert, two Montreal-based computer systems workers, for tying up a government computer for almost an hour in August 1986. Grenier, with the permission of his supervisor Boisvert, used the computer for 57 minutes to develop a personal program.

Liability in Expert Systems

David Chase <rbbb@rice.edu>
Sun, 24 May 87 21:38:55 CDT

Perhaps this is an old problem; it occurred to me a couple of days ago. It seems that there is more and more litigation initiated by people who feel that they have been wronged by someone else's malice, negligence, or deep pockets (ahem). Someone out there already sued Lotus, right?

What happens when an "expert system" is involved? Who gets the blame? The programmer, who designed the system, or the expert(s) who supposedly provided the rules that direct the system? Can you imagine the stream of expert witnesses giving their debugging of the problem? Of course, if the

debugger was faulty....

Another source of fault might be the non-maintenance of an expert system. For example, a new edition of the Physician's Desk Reference is published every year. The new information should be added to the expert system, or else it will get out of date (and lack information on new drugs and newly discovered side-effects and interactions). If the expert system was designed in such a way that maintenance was difficult, then the designer might share some blame, too.

Just thought I'd ask. It sounds like a great opportunity for finger-pointing.
David

> [We've been around this one several times before, although not specifically in the context of "expert systems". The juries are not in yet. Are there any new contributions in the wings? PGN]

Electronic Communications Privacy Act

Dave Curry <davy@intrepid.ecn.purdue.edu>
Sun, 24 May 87 19:24:25 EST

When I got the MIT notice from the SECURITY list, I did a little digging in the law books (Purdue's library is a Federal Depository).

I pulled out a copy of the Act (Public Law 99-508, H.R. 4952) and a copy of Title 18 of the United States Code, which it amends. From this (after a couple of hours of "strike words a through f, insert words g through m" -- I'd hate to be a law clerk), I extracted most of the "interesting" parts of the law.

These parts pertain to administrators and users of electronic communications services (if your machine has electronic mail or bboards, it fits into this category). The parts I specifically went for were what we can and cannot do, what the punishment is if we do it, and what our means of recourse are if it's done to us. I left out all the stuff about government agents being able to requisition things and stuff, and all the stuff pertaining to radio and satellite communications.

So anyway, I typed all this stuff in to give it to our staff so they'd be aware of the new legislation. Since there is probably interest in this, I am making the document availble for anonymous ftp from the host intrepid.ecn.purdue.edu. Grab the file "pub/PrivacyAct.troff" if you have troff (it looks better), or "pub/PrivacyAct.output" if you need a pre-formatted copy. Bear in mind I'm not a lawyer, and I just typed in the parts of the law I deemed to be of interest to our staff.

--Dave Curry

ATM security (from Usenet)

Martin Minow <decvax!LOCAL!minow@decwrl.DEC.COM>

Sun, 24 May 87 19:20:09 edt

[Background: sci.crypt is intended to discuss cryptography issues.
Recently, it has been discussing automatic teller machines, the
security of personal id numbers, and how cards are invalidated after
successive incorrect input of the user's "secret code." This article
branches out a bit, and might be of interest to Risks readers.

Martin Minow]

Path: decvax!ucbvax!ucbcad!ames!lll-tis!ptsfa!lll-lcc!well!shibumi
From: shibumi@well.UUCP (Kenton Abbott Hoover)
Newsgroups: sci.crypt
Subject: Re: ATM security (was Re: DES info wanted)
Date: 23 May 87 21:26:55 GMT
Organization: Whole Earth 'Lectronic Link, Sausalito, CA

The determination on invalidation is done at the host. If the programmer wants
to invalidate the card on three attempts, well, then the programmer has to
put a flag on the data record for the card. An example: Bank Of America (who
I used to work 4) simply sends a report to the branch where your account is
and the branch personel decide whether to flag your card, or just call you
and ask what the h**l is going on.

Trivia: The Diabold and IBM ATMs (diabolds have CRTs with 4 unmarked buttons,
IBMs say IBM on them, if not they have the cash sort of flop out of a slot and
have an open/closed sign on them) are ...wait for it... 3270 devices! They]
actually have PF keys and the whole nine yards built-in.

Usual chain of activity in an ATM:

1) The interaction with the user, screens, etc. is done by some sort of
controller, a Series/1-type (read: VERY STUPID) machine which controls
a whole set of ATMs. The controller normally resides at some central location
and communicates with the ATMs over leased lines.

2) When you do a transaction, the controller tries to queue up a set of
transactions from its other ATMs. It will either succeed or timeout. In
either case, the transactions are communicated to a 37X5 and from there
to a mainframe which runs a batch job to do the transaction.

3) Most banks cannot update the account base in real-time, so the ATM
processor (the mainframe doing the batch run, not the ATM itself) works
from a database containing last nights data corrected with todays transactions.
The transaction you actually do is simply made a memo posting and is
entered into the actual accounts system as if it were a teller withdrawl/deposit
with a note saying it was from an ATM.

MORE TRIVIA: The PIN is not a timing issue (in most systems). Its just that
the whole transaction is usually sent to the mainframe, and that is slow going.

EVEN MORE TRIVIA: Have you ever been cheated out of money by an ATM? If you
were it was most likely an IBM. Go to your branch and report it, and they
(after you fill out the usual form) will credit your account. Save the ATM

receipt, as they normally ask for it. The IBM machines steal like theives, and normally (like in socks in dryers) the money has simply vanished. Diabold ATMs miscount once in a blue moon, AND if you do a transaction that asks for more money than is the the ATM (they dont keep track in most cases), it will give you what it has and debit your account for only that much.

STILL MORE TRIVIA: Dont deposit cash unless it is to a Diabold ATM. Diabold ATMs check the deposit envelope to see if there is anything in it. IBMs dont. The deposit box is opened by two branch officers, and they (normally) wont swipe cash from a Diabold, since it would be hard to claim an empty envelope. However, an IBM machine...

(someone should really write a book on this subject)

Communications Technology Aids Criminals

<ames!sunybcs!kitty!larry@cad.Berkeley.EDU>
Fri, 22 May 87 23:40:12 EDT

I have submitted the following to comp.dcom.telecom, but thought it may also be of interest to RISKS as indicating how advances in communication technology pose a risk to society by facilitating the conduct of criminal activity.

> In a recent article dmt@ptsfa.UUCP (Dave Turner) writes:
>
> The following is from an editorial by Wayne Green in the June, 1987 issue
> of 73 Amateur Radio magazine:
>
> The recent legislation making cellular phone calls illegal to listen in on
> has provided a bonanza for both organized and disorganized crime. It's
> difficult not to laugh over the situation the cellular industry has gotten
> itself into in its blind pursuit of the fast buck.
>
> What's happened is a mass move into cellular by criminals. They buy a
> cellular system, have an unscrupulous dealer alter the electronic serial
> number (ESN) on the built-in programmable IC, which makes calls both
> untraceable and free--a great combo. They tool around town, making calls
> to Pakistan, Columbia, and their Caribbean drug warehouses at will.

I have a few comments to make on this and some related topics which may be of interest to Net readers. My comments are based upon personal knowledge and experience as one who has provided some forensic science consulting services to certain law enforcement agencies for a number of years.

It's sort of interesting to note that it was even easier to implement spoofing fraud in dial IMTS mobile telephone installations, but such fraud has been virtually unheard of. The reasons for this are: much fewer IMTS channels and much fewer IMTS customers than cellular make such fraud extremely conspicuous; most IMTS installations are combined with MTS installations and have a high probability of telephone company (or RCC) operator monitoring.

My personal opinion is that cellular fraud has been encouraged due to "safety in numbers". :-)

> Cellular has turned out to be great for coordinating every kind of criminal
> activity. It's just what criminals have been needing for years-- a
> dependable, free, untraceable, and safe communications system. With a
> combination of pagers and cellular phones, crooks are making a shambles
> of the cellular system--all protected by Congress.
>
> If you wanted to deal in drugs, how better to get orders from your
> customers than by giving them your cellular phone number? There's no way
> to tap a telephone that can be anywhere in a big city, operating through
> different cells as it moves around. And with an altered ESN it's all free!

Progress in telecommunications has unquestionably been of benefit to criminal activity.

Probably the single greatest benefit has been the introduction of call forwarding. This service has been of such great benefit to the conduct of unlawful gambling, narcotics and prostitution operations that for many years I have jokingly referred to it as: "1A Criminal Facilitation Service"; AT&T and BOC people may appreciate the satire in this remark.

As an example, an unlawful gambling operation could change location every day or so, with the telephone number for bettors being the same. This situation also neatly defeats any court-authorized eavesdropping warrant since there would never be conversations on the telephone pair that was the subject of such a wiretap; a forwarded call never takes place on the physical line whose number was dialed. In earlier No. 1 and No 1A ESS installations there was no rapid method to determine to what number a given line had its calls forwarded; such determination could only be made by an experienced switchman using the ESS maintenance tty. This rather frustrated law enforcement agencies in their investigation of unlawful gambling and narcotics activity. Furthermore, I know of some instances where telephone company personnel flatly denied to law enforcement investigators that they could determine the forwarded telephone number; this was, of course, a false statement, but was made in a misguided effort to keep the telephone company "uninvolved".

As an interesting aside, prior to the advent of ESS and call forwarding, some larger unlawful gambling operations used an electronic device called a "cheese box" that effected a rudimentary kind of call forwarding in a manner similar to a loop-around test line. Two telephone lines would be ordered for say, an unoccupied office or apartment, and each line would connect to the "cheese box". The actual location of the gambling operation would call the first line, and remain on the line and wait for calls; the "customers" would call the second line, with the result that it would auto-answer and be connected to the first line.

Telephone company loop-around test lines were used for the conduct of unlawful narcotics dealing during the 1970's, but this practice has generally disappeared as telephone companies: (1) installed 60A control units or equivalent devices that dropped loop-around connections upon the detection of speech energy (legitimate use of loop-around test lines is for single frequency transmission measurements only); and (2) went ESS and therefore had "call trace" capability that would automatically determine the origin of calls to loop-around and other test lines.

After call forwarding, the next most useful communications adjunct to criminal activity is the voice radio pager. It is an unfortunate fact of life that no self-respecting prostitute or "street dealer" of narcotics would be caught without their voice pager. Voice pagers represent an ideal, inexpensive

method of arranging clandestine meetings. A typical voice pager scenario: customer calls narcotics dealer's pager from a coin telephone, giving coin telephone number; narcotics dealer finds coin telephone to call coin telephone where customer is waiting to arrange for a meeting. What could be simpler and more untraceable?

In my travels, I have known of only two instances where criminals used any speech privacy devices (speech scramblers) to defeat eavesdropping (lawful of otherwise); however, I suspect that a new generation of low-cost digital speech privacy devices will result in more of these devices being used by criminals. The units that I have seen used were all based upon analog "speech inversion" techniques; these devices are easy to defeat, whereas the digital devices are virtually impossible to compromise by other than NSA.

One of the most novel (at the time) applications of communications technology by criminals that I have personally seen was the use of telecopiers by a large unlawful gambling operation about 11 years ago. While the law enforcement agencies involved had obtained eavesdropping warrants to install wiretaps on some of the telephone lines involved, they were totally baffled by the strange sounds heard during some intercepted calls. I was called in to solve the mystery, and some listening told me that this was an FSK facsimile machine running in 6-minute mode. So we borrowed a telecopier to decode the tapes; this was not as easy as first anticipated. I finally had to modify the telecopier to start in receive mode without receiving a ringing signal (which was not possible from an after-the-fact tape recording). We got some pretty damning evidence, much to the consternation of the criminals (who suspected a wiretap, but felt that the facsimile machine was "secure"). While telecopiers are rather common today, such was not the case 11 years ago. I suspect that as telecopiers decrease in price, they too will be more commonly used by criminals. While Group I and Group II facsimile machines are fairly easy to monitor, the more common Group III (sub-minute) machines are much more complex since they are digital and require faking a handshake protocol by any receiving machine used as a monitor.

> If it weren't against the law to listen to cellular channels, I'd suggest we
> hams help the law by listening for suspicious cellular calls and recording
> them. Say, how'd you like to get the goods on some serious crooks and find
> (a) the evidence is inadmissible because it was illegally attained and (b)
> yourself on trial for making the recordings. So join me in a big laugh, okay?

I know of law enforcement agencies that have in the past used scanners to listen to paging service channels and IMTS mobile telephone channels, and have obtained useful intelligence information. None of the information so derived was used in court per se, but it may have contributed to the "probable cause" for looking in a certain _public_ place at a certain time. When any investigator was pressed in court for the "basis of probable cause", the information was attributed to an "anonymous informant" - a VERY common source of law enforcement information. Under the circumstances, I see nothing wrong with this - but I am certain that a number of people will disagree with me.

For example, an experienced investigator can readily detect a drug deal going on via certain types of pager messages. Now, if a police cruiser just happened to be going by the aforesaid location, and decided it was time for a routine traffic check... :-)

[Flames about prosecuting people for alleged "victimless" crimes such as gambling, narcotics and prostitution should be directed to /dev/null]

<> Larry Lippman @ Recognition Research Corp., Clarence, New York
<> UUCP: {allegra|ames|boulder|decvax|rocksanne|watmath}!sunybcs!kitty!larry
<> VOICE: 716/688-1231 {hplabs|ihnp4|mtune|seismo|utzoo}!/

Search RISKS using swish-e

THE RISKS DIGEST

Forum on Risks to the Public in Computers and Related Systems

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

Volume 4: Issue 91

Thursday, 28 May 1987

Contents

Electromagnetic Interference (in Japan)

"Lindsay F. Marshall" <lindsay%kelpie.newcastle.ac.uk@Cs.Ucl.AC.UK>
Thu, 28 May 87 9:40:09 BST

CHIPS ARE DOWN OVER ELECTRONIC POLLUTION (The Guardian, 26 May 1987)

Japan is engulfed in an "electronic smog" which has caused deaths and injuries, and jammed an airport radar system, according to recent findings.

Electronic smog occurs when electromagnetic waves from equipment like personal computers and electronic game machines "escape" and trigger other machines. An electromagnetic wave can also be caused by a mere spark. An electric spark from a crane operating in a valve plant set off a lathe-operating robot in 1982 killing an assembly-line worker.

A simple household device like a television aerial booster can have dire consequences. Osaka International Airport's radar screens were jammed by electromagnetic waves from a nearby television aerial booster. The fault and its cause were discovered. But the Ministry of post and Telecommunications (MPT), which has set up a group to investigate the problem, admits that an air crash could have occurred.

Forty-two people were injured last September when two cars on a roller-coaster crashed. The MPT suspects electromagnetic waves from an unknown source were to blame. It says that communications at a busy railway switching point have been jammed by waves from television game machines. Train doors have inadvertently opened several times. The MPT wants manufacturers to redesign their electronic goods so that the waves cannot escape.

Lindsay F. Marshall, Computing Lab., U of Newcastle upon Tyne, Tyne & Wear, UK
JANET: lindsay@uk.ac.newcastle.cheviot ARPA: lindsay%cheviot.newcastle@ucl-cs
PHONE: +44-91-2329233 UUCP: <UK>!ukc!cheviot!lindsay

[Remember the item in RISKS-4.89 attributing at least six Japanese robot-related deaths to electromagnetic interference. PGN]
[[By the way, Lindsay's message said "lather-operating robot". As this case was not a close shave, I assume it was a typo.]]

Risk of Inappropriate Technology to Prevent Password Overwrite

<Stachour@HI-MULTICS.ARPA>
Thu, 28 May 87 07:52 CDT

In Risks Digest 4.86, PGN comments on the over-long password, and the article by Bill Young in IEEE Symposium on Security and Privacy, April 1987. I agree that most of us do a bad job of mapping our specifications to our implementations, and Bill does an excellect job of pointing out one way to overcome this risk.

However, I believe that the case Bill points out is but one case of a very general problem that has been solved in a different manner, in a much less risky way. Specifically, the specification that was violated in the implementation can be summarized as "A data area is overwritten by a method that should have no access to that data area." This over-writing problem is quite general: it happens for arrays (such as when strings are implemented as array of characters), for improperly based structures, and other places.

The particular error cited by Bill Young could not have happened if the implementation had been in a language such as PL/I or Ada, where over-running the bounds of an array is a required run-time check (in the cases where the compiler cannot determine at compile-time that the assignment is not 100% safe) instead of in a language like C where all the

effort is on the programmer, and no help is given to her by the language. Such checks are clearly not new technology, since Multics (written in PL/I) has been doing such for over 20 years. Nor is the technology new to hardware, since the Burroughs B5500-series and MCP (written in Algol) has also been checking for a similar period.

One of the reasons for the reliability of Multics and MCP is that they do NOT depend on perfect programmers, but use both the language run-time (checking software descriptors) and hardware (segmentation, rings, ...) to check for common overwrite errors and other access violations.

I would personally prefer to put my faith in a compiler generating correct code and the run-time for the language checking descriptors properly than putting my faith in every coder of every array-reference in every program, even where all such programs have been "proved" to be correct, simply due to the sheer size and difficulty of such proofs, and the high probabiliy of an error in the proof, or in the configuration-control of different versions (one proved correct, a different one installed) of the software, or some other error that makes the proof "non-valid".

This leads to my question:

What RISK do we bring on to ourselves (both personally and professionally) when we ALLOW inapproprate technologies to be used (or in many cases, forced by others) that thereforce create unreliable, non-robust software, when both the hardware and software technology to prevent many of the problems have existed long enough that every reasonable person working in software should be aware of them.
[I know that many people today only study the things of the current generation, done simply and incorrectly for simple systems, and don't understand much else, but that's another question.]

Paul Stachour, Honeywell & University of Minnesota, Stachour@UMN-CS.EDU

Passwords and Statistics

<Boebert@HI-MULTICS.ARPA>
Tue, 26 May 87 10:50 CDT

From the Computer Shopper, May 1987:

Password Snatcher -- RS-232 Data tap. Lets you actually "see" the data being sent or received on an RS-232 line. Connect a terminal or microcomputer to the tap connector to capture data, or connect a serial printer to get a hard copy. Jumpers allow for routing TD, RD, or both to the tap. $29.95.

[Great jumpers. A Computershopper must be like a grasshopper. PGN]

Re the statistics on use of opposite-sex names for passwords: The best rebuttal to this kind of statistical argument came from the redoubtable John W. Campbell: The laws of population growth tell us that approximately half the people who were ever born in the history of the world are now dead. There is therefore a 0.5 probability that this message is being read by a corpse.

Why Cellular phones at the Indy 500?

Robert Adams <adams@littlei.UUCP>
Tue May 26 15:00:45 1987

While watching the Indianapolis 500 on TV this Sunday, I saw them do a feature on one of the car crews that were using a celluar phone to talk to the driver on the track. You see, most crews use some sort of CB or shortwave set to talk between the pit and the driver and the TV announcers are always talking about what they overheard on the radios. This one car had a celluar phone and the crew would phone the driver to discuss things. This seemed really strange to me until I realized that the use of the phone meant that no one could legally listen in on their conversations.

Everyday someone discovers a new way to use that law.

Robert Adams, Intel Corp., ISO Systems Development, Hillsboro, OR

Information Security Products and Services Catalog by NSA

"Kurt F. Sauer" <ks%a.cs.okstate.edu@RELAY.CS.NET>
Thu, 28 May 87 3:09:56 CDT

RISKS Readers who have a professional or personal interest in information security on a practical level might be interested to learn that I have just received my copy of the April 1987 Information Security Products and Services Catalogue, prepared by the National Security Agency. There are no protective markings on the document, and (since they're VERY CLEAR when things *aren't* public-domain) I presume it is available on request by writing to

Director, National Security Agency, 9800 Savage Road,
Fort George G. Meade MD 20755-6000

Anyway, it's in interesting compendium of companies who provide communications and information systems security devices and services. According to some accompanying document(s), "...this catalogue will be distributed quarterly to [organizations] who received [certain lists] previously... Plans are under way to request that they be provided through the Government Printing Office on a subscription basis."

The document is in 5 parts and lists companies and equipments thus:

(1) Endorsed Cryptographic Products List
(2) NSA Endorsed Data Encryption Standard (DES) Products List
(3) Protected Services List
(4) Evaluated Products List
(5) Preferred Products List

Also included is a brief, but informative, description of categories of information which requires security, information about purchase and restrictions on the purchase of these devices and services.

Happy hunting! Kurt F. Sauer, Director of Operations, Decision Studies Group, Inc./OP, Post Office Box 701318, Tulsa, OK 74170-1318, Tel +1 918 749 0893

Re: TRW "Credentials"

John R. Levine <johnl@ima.ISC.COM>
Mon, 25 May 87 12:57:07 EDT

Ron Heiby wrote in RISKS-4.89 about a report in Insight magazine on TRW's new "Credentials" that gives you access to your TRW credit record for $35/year.

The current issue of Forbes also reports on this new so-called service. Forbes points out that TRW is required by law to provide a copy of one's credit record for free any time credit is denied because of a credit report, and for a nominal reproduction fee at any other time. They express incredulity that people seem willing to pay $35 for what they could already get for free. In addition, TRW encourages the Credentials customers to add extra information voluntarily to their credit records under the dubious theory that this will help them to get credit in the future. People seem to think that because their info is in TRW's computer it will be more credible.*

John Levine, ima!johnl or Levine@YALE.somethingorother

* - Not a pun, no matter what you may think.

More on the Stark

Peter G. Neumann <Neumann@CSL.SRI.COM>
Tue 26 May 87 11:25:41-PDT

An article by Molly Moore of the Washington Post appeared in the SF Chronicle, 26 May 1987, pp. 13 and 14. It adds lots more details on the Stark and its equipment. The computers were programmed to give a LOUD alarm that the missiles had been launched, even when NOT in the mode to fire the Phalanx automatically. Perhaps the radar scans only in the direction that the Phalanx was pointing? (We have already noted reports that the computers were not even working at the time, although there is also a denial by the Captain.) On the other hand, the fact that the use of computers in this context for automatic firing of the Phalanx is deemed unsafe is of great interest to RISKS. Reliance on continual preparedness in the defensive use of unreliable systems with unprepared personnel seems quite risky.

> [Thus the next item is relevant, for further background. However, let me again remind contributors to cite your references carefully. I have rejected a few items that say "I vaguely remember seeing somewhere that ... ." Also, please try harder to avoid wild speculation.]

Phalanx Schmalanx

Mike Trout <rpics!brspyr1.BRS.Com!miket@seismo.CSS.GOV>
28 May 87 21:22:33 GMT

Regarding the recent USS Stark incident, much has been written about the Phalanx anti-missile system mounted on the ship. Generally, Pentagon spokespeople--parrotted by the news media and net posters--have stated some variation of the following:

"If only {choose one or more of the following}:

A) the Phalanx had been switched to "automatic"
B) the ship's stern, where the Phalanx is mounted, had been pointing toward the incoming missile(s)
C) the crew had been alert/warned in time to properly use the Phalanx
D) the Phalanx had been operating properly (crew allegations of assorted Phalanx malfunctions/down time/maintenance problems)

then the Phalanx would have easily blown the incoming missile(s) away and we would all live happily ever after."

This universal faith in the Phalanx is a dangerous belief that I take exception to. Contrary to the way the Navy and the media talks, Phalanx is a very new weapon that has NEVER been used in combat conditions.

History tells us that military hardware testing conditions and combat "real world" conditions probably don't even lie in the same universes. US military hardware testing, driven by profit motives and military career advancement, is particularly atrocious. Everything I've ever discovered about this situation leads me to believe that to get a good idea of how a weapon will really perform, the best strategy is to utterly IGNORE test results.

The things that the "military-industrial complex" (MIC) (why is that a taboo term these days?--Eisenhower coined it) will do to test a weapon are truly bizarre. Drones (moving at the breakneck speed of 60 mph, without evasive action) have been painted with gloss red enamel to absorb more laser energy, to "prove" that lasers can shoot down planes. Gigantic aluminum foil bull's-eyes have been arranged on the ground so that the Pershing II's radar could find its target. Over 160 mobility tests of the M1 tank resulting in the tank's breakdown were thrown out as "invalid", while the single test in which the tank didn't break down was presented as the final result. Every single test of the GLCM cruise missile has been altered to cover up grossly unacceptable navigational errors.

Most of the Phalanx testing data I'm aware of shows excellent results, usually on the order of 80% of incoming targets hit. But as I've stated before, that may mean nothing at all. One problem in the Phalanx testing the MIC doesn't like to talk about is that even if the incoming missile is hit, the hit takes place so close to the ship that the ship is still blasted by the missile's wreckage. The Phalanx's MAXIMUM range is only about 1.5 miles, and most anti-ship missiles cover that distance in just a few seconds. This problem becomes worrisome when you consider that of the four Exocets that hit British ships off the Falklands, THREE were duds, including the one that hit the HMS Sheffield. But the devastation caused by a dud

missile was still severe enough to wreck or sink the ships hit. Even without an exploding warhead, an anti-ship missile is a large, heavy object travelling at high speed carrying fuel tanks at least partially filled with various formulas of highly volatile rocket fuel. The force of the missile mass times its velocity is transferred as heat to the ship, resulting in the possibility of a devastating fire--the greatest danger to modern warships. Even if an incoming missile is exploded by the Phalanx, most of the missile's mass will still strike the ship. The mass will, of course, be dispersed by the explosion--the amount depending on how close to the ship the missile was when the missile exploded--and the velocity will be reduced as well. Hopefully this will be enough to save the ship, but even so a ship peppered by high speed flaming debris may be out of action for some time.

Also, remember that the Exocet is a fairly old design as anti-ship missiles go. Most of the newer designs are faster, have better guidance, and might not be duds. The new Soviet SS-N-22 supposedly almost hides behind wavetops while travelling at better than double the Exocet's speed.

The Phalanx's gun--a 20mm gatling--is an excellent, proven weapon that has performed extremely well in real world plane-to-plane combat. But plane-to-plane combat is a different environment than ship-to-missile combat. I've never heard of a pilot shooting down a missile coming at his plane with a 20mm gatling, or with any other weapon for that matter. Years ago, the US Army had a weapon called the "Chapparal", which was a 20mm gatling mounted on an armored personnel carrier. Admittedly, there weren't many opportunities to try it out against enemy air, but it died a quiet death. I know some Army commanders complained about its short range and high ammunition consumption.

This Phalanx faith also makes me worry about the AEGIS cruiser idea. The AEGIS is crammed with all kinds of anti-air and anti-missile stuff, including multiple Phalanx systems, and nearly everybody thinks of it as being able to instantly produce an inpenetrable shield. But I can't help thinking about an interview with the Second Fleet commander a couple of years ago. He said if a real war broke out, he'd send all his AEGIS cruisers home. He contented that its high-powered radar, tracking, ECM, and weapons control electronics puts out such a blatant electromagnetic signature that it would attract every Soviet plane, ship, and sub within hundreds of miles. Sort of like a bug light that attracts so many bugs that despite its excess power, it can't kill the bugs fast enough and it clogs and shorts out.

So let's not get carried away by the Phalanx. It wasn't supposed to be a perfect missile defense system, but the MIC has to justify all that expense. It's probably useful as a last-ditch emergency measure, but thinking of it as a missile umbrella leads to a "crutch mentality" that neglects more useful missile defenses like air cover, anti-AIRCRAFT weapons, electronic countermeasures/chaff, and evasive action.

Michael Trout (miket@brspyr1) =-=-=-=-=-=-= UUCP:ihnp4!dartvax!brspyr1!miket
BRS Information Technologies, 1200 Rt. 7, Latham, N.Y. 12110 (518) 783-1161

Re: Stark

Torkil Hammer <sdcsvax!sdcrdcf!psivax!torkil@ucbvax.Berkeley.EDU>
Tue, 26 May 87 13:33:17 PDT

American commentators have the curious notion that, when English-speaking soldiers die, it must be explained as a result of human errors, but when their foreign speaking counterparts go the ultimate way of soldiers, it is considered a victory. Compare the newsmedia coverage of the Sheffield and Stark incidents with the Libya and Grenada ones.

It looks to me, that the only risk involved is one of messing with guys packing Exocets, and ramifications depend on what language you speak.

The technical discussion in this newsgroup has barely mentioned that Exocets are smart missiles with an unusually high rate of 'success', as seen from the launching end. Which translates to an equally high rate of 'failure' as seen from the targets.

So a technical discussion on the failure of the ships' defenses must logically be followed by a discussion on why the second missile arrived without exploding. Rather atypical for Exocets. Usually they do. Computer failure?

torkil hammer, Pacesetter Systems Inc., Sylmar, CA

Laser guides (RISKS-4.90)

"Jon A. Tankersley" <apctrc!zjat02@seismo.CSS.GOV>
27 May 87 14:57:43 GMT

Seems to me that the laser guided technology is about the same as the wire guided technology of the Arab-Israeli War. Wire guided TOW missles could be easily defeated by spraying the general direction of origin. Many Israeli tanks ended the war with lots of wires draped over them.

The only 'smart' way that weapons can work is by adding intelligence, but that can even cause problems (Berserker SF series by Saberhagen, etc.)

-tank- Amoco Production Co, Tulsa Research Center [Tanks.]

Re: Risks of running Risks ["One" the record]

<Jeff Woolsey <woolsey@nsc.NSC.COM<>
Tue, 26 May 87 09:47:16 PDT

```
 >    After 14 days (326 hours), your message has not yet been            |
 >fully delivered.  Attempts to deliver the message will continue         |
 >for 178956963 more days.  No further action is required by you.         V
 >   [********* = = = = = = = = = = = = = = = = = = = = = = = = = = = = !!!!
```

That number is 0xAAAAAAA _+ 7 (1 week). Even the machine shrieks in astonishment at having to keep retrying that long.

Jeff Woolsey National Semiconductor Corporation
...!nsc!woolsey -or- woolsey@nsc.COM -or- woolsey@umn-cs.ARPA

Re: Risks of running RISKS (RISKS 4.88)

Will Martin -- AMXAL-RI <wmartin@ALMSA-1.ARPA>
Tue, 26 May 87 15:45:47 cdt

It was mail to me that generated that erroneous mailer barf message that told you it was going to keep trying for 178 million-odd more days...

Sorry about that... Our net-host 750 has a flaky clock, even though it keeps getting parts replaced by maintenance, and in that instance it crashed briefly and came up with a system time thirteen days in the future. Since, at the same time, our main user machine had been down and mail to it was sitting in the queue on the 750, the mail process on the 750 thought it was two weeks since they had been queued and so merrily generated a great spew of garbage mailer messages. I still don't know what is causing them to have that enormous number of days displayed. We get all sorts of strange numbers showing up in that field...

Anyway, when I noticed this, we cut off outgoing mail and I did a mass delete of all message traffic with a "Waiting mail" subject line. Unfortunately, it appears some slipped out before we caught them. Sigh...

If you see any again, please ignore them. (Though I'm sure you don't need any more junk mail like that cluttering up your inbox.)

Will Martin

Re: Computer thefts (re: RISKS-4.82)

David Phillip Oster <oster%dewey.soe.Berkeley.EDU@Berkeley.EDU>
28 May 87 23:52:27 GMT

Apple computer sells a thing called a "security kit" that permanently attaches a steel shackle to a Macintosh and Keyboard. With a steel cable passing through both shackles, and padlocked to a water pipe, it makes the Macintosh hard to steal. (Good for students.)

I don't know whether this feature was preserved in the new Macintosh SE and Macintosh II, nor what it costs.

The security kit does not protect the mouse, which can be easily unscrewed and walked off with, but it should help cut down thefts of the whole machine.

Many third party vendors sell kits to lock computers down. Most work by permanently fastening a baseplate to the desk under the machine with a tough

adhesive. Apple's version at least will not ruin a student's dorm's desk.
-- David

[I hate to think of the flood resulting when
someone decides to cut the water pipe. PGN]

Search RISKS using swish-e

THE RISKS DIGEST

Forum on Risks to the Public in Computers and Related Systems

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

Volume 4: Issue 92

Saturday, 30 May 1987

Contents

Computer matching of cats and dachshunds

Kuhn <kuhn@ICST-SE>
Fri, 29 May 87 10:33:57 edt

Charles Osgood reported the following story on CBS Radio this morning:

Hundreds of cat owners in Chicago received a bill for five dollars accompanied by a letter explaining that they were required to register their dachshund. Apparently the Cook county health department had provided rabies shots for pets and kept a computerized list of animals receiving shots. Someone got the bright idea of matching this list against the list of dogs licensed in Chicago to find dogs that received shots but were not licensed. Cats are not required to have licenses.

Unfortunately, the county uses the code "DHC" to represent "domestic house cat", while the city of Chicago uses "DHC" to represent "dachshund", resulting in computer generated form letters to the owners of the "DHCs". After the mess was discovered, a city official said "I guess if we'd thought about it, we would have wondered why there were so many dachshunds in Chicago." (not an exact quote, I couldn't take notes when I heard the story.)

Rick Kuhn, National Bureau of Standards

[Perhaps some of us should keep tape recorders in our cars, in the interests of accuracy... <Chicago is trying to rein cats and dogs?> PGN]

Electromagnetic Interference (EMI) & Liability

<Richard.S.D'Ippolito@sei.cmu.edu>
Friday, 29 May 1987 12:16:34 EDT

In RISKS 4.91 and some previous digests, some attention is drawn to the problems of equipment malfunctioning due to EMI. I spent my early career years designing electronic control equipment which was applied in very (electrically) noisy environments, such as steel mills and forge shops. The equipment was used to control the electrode gap spacing on various types of melting and refining furnaces, such as electric arc furnaces operating at 400 volts and 30,000 amperes. The early designs contained mostly analog circuits, which were supplemented by the then new digital technology. In one of these environments, where RF was used to melt artificial ruby for growing laser crystals, a Simpson VOM would read without the leads connected and oscilloscope use was impossible. We now have a new generation of designers without practical experience in analog circuits, noise filtering, and shielding techniques, who don't think of voltages and currents, but only of zeros and ones. While I agree with the FCCs EMR regulations, they attack the problem only from one side. We must urge designers to submit the equipment to operational tests under reasonably expected EMR fields, as the cranes and even common static electricity can never be eliminated. And those of us who use EPROMS shouldn't forget that light (even the flashlight of an unsuspecting service man) and X-rays are EMR. We may soon find the government forcing certification at the emissions-receiving end. And the liability laws are such that you could have a hard time defending the use of a single PROM in a critical application if an erasure caused by cosmic radiation caused an accident.

And some day, I know, just the right EMI will come along and cause everyone's

digital watch alarms to sound at once, thus deafening us all.

Richard S. D'Ippolito, PE, Software Engineering Institute, Carnegie Mellon University, rsd@sei.cmu.edu. (412)-268-6752.

Horror story about inadvertent wiretapping

Gordon Davisson <gordon@june.cs.washington.edu>
Fri, 29 May 87 23:19:34 PDT

In RISKS DIGEST 4.91, Boebert@HI-MULTICS.ARPA (Earl Boebert) writes:
> From the Computer Shopper, May 1987: Password Snatcher -- RS-232 Data tap.

You don't need any special equipment to do this. I once accidentally put an extra null modem (a receive/transmit channel swapper) between the VAX and the Macintosh I was using as a terminal. This meant the Macintosh was listening to a wire that wasn't being driven at the other end. With a normal terminal, this wouldn't have done anything interesting, but Macintoshes have unusually sensitive receivers, and there was enough crosstalk in ~150 ft of twisted pair cable for me to get a complete (error-free!) transcript of everything going through that cable. This happened to include somebody's password...

(Just thought I'd give the security-conscious people out there one more thing to worry about.)

Gordon Davisson (gordon@june.cs.washington.edu) (uw-beaver!uw-june!gordon)
Computer Science Department, University of Washington. Seattle, WA, 98195.

ATM fraud

Bob Johnson <U18323 at UICVM>
29 May 1987 09:48:55 CDT

In the past few days some of the Cash Station (*) ATMs in the Chicago area have changed the format of the receipts they dish out. The new style no longer has the account number of the account used in the transaction.

The above was a statement, now I have a question.
Has anyone heard of the 'new' phone features 'Call blocking' and 'Call tracing'? Supposedly call blocking will not let your phone ring if call is placed from a certain number (number to be designated by you, from the phone which you are at) and call tracing traces a phone call after one presses a certain key sequence (on your phone). I've heard that these are available in California and another area. Is there truth in this?

Bj

* I'm sure this is a registered trademark for someone

Computer thefts (Risks 4.91)

<Mike_Alexander@um.cc.umich.edu>
Fri, 29 May 87 13:31:58 EDT

The Public Facilities people at the University of Michigan Computing Center use the Macintosh Security kit mentioned in Risks 4.91 to protect Macs installed in public areas. They modified it to protect the mouse too, and now they find that people steal the tracking ball out of the bottom of the mouse. Someone jokingly suggested epoxying it into the mouse, but so far they haven't resorted to that.

[Epoxy on both their mouses. PGN]

Re: Computer thefts (re: RISKS-4.82)

Brint Cooper <abc@brl.arpa>
Fri, 29 May 87 10:10:21 EDT

Perhaps I missed it, but I haven't seen anyone mention the kits for under $40, sold by 3rd parties, that permanently attach to two or three parts of your computer and attach to one another by a tough steel cable that can be passed through a radiator (here in the East), wrapped through a hole in immovable furniture, or attached to something immobile.

We bought my son's at ComputerLand, but they're available all over by now.
_Brint

Shooting Down Exocet Missiles

Mark S. Day <MDAY@XX.LCS.MIT.EDU>
Fri 29 May 87 11:50:22-EDT

This morning's Boston Globe included an article on the Phalanx and Aegis defense systems. The analysis was that the Stark was out of luck, because the Phalanx couldn't possibly have shot down the Exocet. It was possible that an Aegis system could have shot down the missile, but the article said there had been only two even-close-to-meaningful tests and they weren't all that impressive. In the first, the Navy classified as "sea-skimming" any missile that came in at an altitude of 100 feet or less above the waves. This let them shoot down a missile at 100 feet, which is pretty irrelevant when it comes to an Exocet at 10 feet. The other test involved shooting down an Exocet (at 10 feet above the waves) but with the Aegis system mounted on a barge so that its radar was at approximately sea-level. The problem that both tests successfully avoided was having to look down at the radar reflections off the wave tops. The conclusion of the article was that in all likelihood the Aegis couldn't have distinguished an Exocet from the "sea clutter".
--Mark

---

lorenzo strigini <procis%ICNUCEVM.BITNET@wiscvm.wisc.edu>
FRIDAY 29 May 1987 10:45:57 SET

(IEI - CNR;Via S.Maria 46;56100 Pisa;Italy)(Tel +39 50 43023)
To: <risks@csl.sri.com>
Subject: Phalanx is unreliable?

In RISKS 4.91 I read:
... the use of computers in this context for
automatic firing of the Phalanx is deemed unsafe ....

As I understand the situation, the problem in question is not peculiar to computer technology: if you carry a handgun, you do not keep it always ready to fire, except in the case you are in a very dangerous situation, and then you accept much higher risks of hurting somebody by accident. There is no such thing as a safe weapon: one has always to decide which compromise between security against enemies and safety from your own weapon is best at the moment. The difference between Phalanx and revolvers is not qualitative ("using Phalanx is unsafe").
Just for accuracy (and, I am not sure the previous poster had made the mistake I thought I saw, but I thought saying this may be useful anyway). Apart from this, discussing how good radars and computers may be for telling friend from foe is certainly interesting.

Lorenzo Strigini

Stark Incident

Eugene Miya <eugene@ames-nas.arpa>
Fri, 29 May 87 11:31:17 PDT

I was on vacation when the Stark incident happened, and am just catching up. Upon reading some accounts, I think inappropriate attention is being focused on the Stark's defensive systems. What concerns me more was the role of the AWACS aircraft and the look-down radar it carries. (I note American crews.) It appears from accounts I have read that it was the maneuver of the plane that gave away the launching of the missiles, not any radar returns from the entire minute in missile flight. I don't know the range, but it seems the sea state was ideal for detecting low flying cruise missiles of this type (easier than terrain), and should have given a full minute warning. The failure of the USAF AWACS to report sooner might show flaws in the integration of the C^3I of the region making "layered defense" a joke. I don't know the AWACS radar system (like frequency, range from target (The F-1), etc.), and I hope that this aspect of the investigation is not lost to Adm. Rogers. I no longer work with radar.

The stuff on the net focusing on the lack of a "front" Phalanx is probably a little misdirected. These missiles come in from the side (since the cross-section of a ship is larger and armored ships have less side armor) and the system on the Stark is probably adequate for such side protection. If the Phalanx were in the front, and the missile had hit more aft, there probably would have been outcry for protection in the stern. The readiness state was still the important thing in the end.

In the end, the title of the old WWII British movie sums up the role of this type of ship: They Were Expendable.

--eugene miya

[Thanks. Once again, RISKS has had much speculation on this subject. We now have a lot of background with which to understand the conclusions of the investigation, so let's slow down for a while. PGN]

Technical error in item "Phalanx Schmalanx"

Mark Brader <msb@sq.com>
Fri, 29 May 87 23:49:31 EDT

Mike Trout writes:

> But the devastation caused by a dud
> missile was still severe enough to wreck or sink the ships hit. Even
> without an exploding warhead, an anti-ship missile is a large, heavy object
> travelling at high speed carrying fuel tanks at least partially filled with
> various formulas of highly volatile rocket fuel. The force of the missile
> mass times its velocity is transferred as heat to the ship, resulting in the
> possibility of a devastating fire--the greatest danger to modern warships.

In fact, of course, the amount of energy transferred to the ship is proportional to the missile's mass times the SQUARE of its speed. Knowing only how big an Exocet is and how much a V-2 weighed, I'll guess the weight of the Exocet at 1/3 that of a car. According to Newsweek, it moves at 500 mph. So imagine being hit by a car going at 50 mph. The missile would deliver over 30 times that much energy from impact alone!

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

Phalanx (Re: RISKS-4.91); Laser guides (RISKS-4.90)

Phil Ngai <amdcad!phil@decwrl.DEC.COM>
Fri, 29 May 87 16:22:51 PDT

Unsafe does not imply unreliable. A loaded gun is unsafe to carry around, but that does not mean it is unreliable in the sense of "will it fire when I pull the trigger". The Phalanx shoots at anything that it sees. You wouldn't normally arm it unless you were in combat.

>From: "Jon A. Tankersley" <apctrc!zjat02@seismo.CSS.GOV>
>Seems to me that the laser guided technology is about the same as the wire
>guided technology of the Arab-Israeli War. Wire guided TOW missles could
>be easily defeated by spraying the general direction of origin. Many
>Israeli tanks ended the war with lots of wires draped over them.

That works if the laser designator is operated by the launch crew. One of the advantages of laser guidance is that the designator can be operated by a

separate crew in a location which the target has trouble figuring out. The launch crew can run as soon as the missile is launched.

The FOG-M is also a major advance in this type of technology.

Phil Ngai, {ucbvax,decwrl,allegra}!amdcad!phil or amdcad!phil@decwrl.dec.com

---

Laser guided anti-tank weapons

Eugene Miya <eugene@ames-nas.arpa>
Fri, 29 May 87 11:38:50 PDT

Jon Tankersley compares wire-guided munitions to laser designated. No, they are a new-generation weapon. The laser designator need not be located at launch point and in fact it is preferable they be at different points. His suggestion of smart weapons is more scary for me, don't.

Just noted: Hammer's comment about Exocets not exploding. Actually, duds happen all the time. There were several duds in the South Atlantic. Actually probably makes disarming them easier.

--eugene

---

unfair testing

<PPeters@DOCKMASTER.ARPA>
Fri, 29 May 87 15:43 EDT

A discussion in RISKS 235 relating to the STARK incident and the "MIC" test procedures stated "Drones...have been painted with gloss red enamel to absorb more laser energy." The implication was that this is an unfair advantage. Unless these are heat seekers, I would think that the advantage would be obtained by painting them to REFLECT more laser energy.

"Credentials", Privacy, etc. (Re: RISKS-4.91)

<willis@rand-unix.ARPA>
Fri, 29 May 87 09:55:06 PDT

As a member of the computer fraternity who who has been in the privacy area for a long time (e.g., chaired the HEW Committee whose report led to the Federal Privacy Act, member of the Privacy Protection Study Commission), I'd like to offer $0.25 more on the subject of TRW's Credentials. To me, this is marketing of the obvious and of information that is largely useless for most people. I didn't see Forbes on the issue but it seems that it expresses the same view.

In the course of various privacy activities, I've had occasion to talk in depth with TRW Credit Data and see my own record -- one time for free and another time for (I think) $7.50. For anyone that is seriously thinking of

subscribing to Credentials, I'd urge that you invest the nominal amount first and see how little is really in your record. All of the good things that you've done creditwise (e.g., regular mortgage payments for 30 years) will not be there; if you've been too bad (e.g., declared bankruptcy) it will be there. Even then, bankruptcy records have a legal life of 7 years, at which point TRW is obligated to expunge the record. Beyond that your record will be mostly a listing of your credit card accounts together with a comment about outstanding balance or being current. As I recall when I last looked, my TRW credit file had about 6 entries in it although I held many more plastic cards than that and had much other credit activity. Your SSN may be there, although TRW is not authorized under any law to solicit its collection.

So, take a test flight with your record before plunging into a $35 annual fee.

The things (as I recall the blurb) that Credentials offers is a regular copy of your record and notification of whenever the record is consulted. I believe TRW does not offer to tell you when the record is updated on existing lines of credit. Unless one is extraordinarily active in creating new credit accounts or in hunting new jobs, your record will not be consulted very often and so you won't hear much. Meanwhile for less than $10 a throw, you can get your record once or twice a year directly -- if you're interested enough to want to know that often. If you want to know something about how your credit record plays a role in activities that you may not suspect (e.g., investigations of various kinds), one can get some insight for a year's subscription.

It isn't TRW that represents the really big risk to most people. It's the small local credit bureau tucked away on some side street, that is frequently manual or at least not extensively automated, and that often engages in information collecting activities that can be a little less than ethical. For example, there is the instance of an individual being hired to poke through a bank's trash in the dumpster; he was picking out "pieces of yellow paper" which turned out to be unneeded copies of delinquency notices on various individual bank accounts. The local credit bureau was learning about delinquencies before the account holders even knew it. In this instance, it was poor information security in the bank that created the risk to individuals.

But the Credentials offer does raise an interesting philosopical point for the citizen. In my own consideration of the privacy issue as it may emerge in the future, I've about decided that each of us will largely have to take of himself. There will be some law and some protections, but the risks of living and operating in a highly automated information society will have to be offset by our own individual protective efforts. We're already being told that the patient will have to play a bigger role in managing his personal medical care; so it's going to be more of the same in privacy and perhaps elsewhere.

Give such a premise, the next question is: does one want to run open loop or closed loop? Does one want to monitor the flow of his automated data as it swirls around? Or just hopefully have things arranged so he knows when negative or harmful events happen? There are some people who want to be proactive and will want to run closed loop; and for them, services like Credentials can be helpful. I suspect most people will opt for open loop, simply because of the burden of watching all the reporting; BUT at the same time, we will all expect mechanisms to trigger negative events to our

attention. Thus, the present Fair Credit Reporting Act requirements of providing a copy of the credit report which reputedly is behind a negative credit action is both appropriate and useful.

But, the initiative still is with the individual; there is nothing automatic about the law's protection against risk. As I recall the law, the organization that makes a negative credit decision is required to tell the individual where it got credit reports that entered into the decision. The individual must then contact such places and request the credit reports. I'm not sure that Forbes is correct about providing free copies; I suspect that the only legal obligation is to make the credit record available for perusal at a specified place of business and during specified business hours. But then the FCRA was ammended I think, and free copies may indeed be a legal obligation. I think that the individual must bear the cost of any reproductions.

On the other hand, I can understanding TRW choosing to send a copy as a business convenience. Among other things, it will avoid having people turn up [at] the front door of an installation whose physical location TRW properly wants to keep secret as an aspect of good system security.

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

TRW's Credentials

Alan R. Katz <KATZ@venera.isi.edu>
Fri 29 May 87 14:26:22-PDT

I have been a member of this for over a year and am pretty satisfied with it.

Advantages:

1. The biggest is that you get notified automatically if ANYONE accesses your credit history. This alone is worth the $35/year to me (it may not be to you).

2. Free copy of your credit report whenever you want. It is true you can get a free copy whenever you are turned down for credit (sometimes a big hassle though). However, the NOMINAL charge for a copy otherwise is $8.00. This can add up if you get more than one a year.

3. "Standard" forms for disputing and correcting information (a little easier than writing letters). Also, since you are a paying customer, you get a little better service.

4. Credit card registration and protection service (generally costs about $12/year elsewhere).

Disadvantages:

1. If YOU WANT (not required), you can tell them income and asset

information which they keep on file along with your credit history.
Then, theoretically, you can apply for a loan or other credit just
by giving your TRW Credentials number and not having to fill
out long applications every time. In practice, I have not
found anyone who will do this (yet) (except for some car dealer whose
ad was sent as a part of the TRW Credentials package!).

2. $35 / year

All in all, it's worth it if you want to know when someone accesses your credit history (which they are NEVER supposed to do unless you authorize it) or if you want to get more than one or two credit reports a year.

Alan (Katz@ISI.Edu)

Search RISKS using swish-e

Report problems with the web pages to the maintainer

Search RISKS using swish-e

THE RISKS DIGEST

Forum on Risks to the Public in Computers and Related Systems

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

Volume 4: Issue 93

Mon 1 June 1987

Contents

Soviet Air Defense Penetration [Red Square Dance?]

Fri, 29 May 87 11:43:05 PDT

Around 7:30 p.m. on 28 May, a white single-engine Cessna with West German markings buzzed Lenin's mausoleum and landed near the Kremlin wall on the 750-yard-long Red Square in central Moscow. The pilot was a West German teenager named Matthias Rust. The plane had flown 550 miles from Helsinki to Moscow across ``one of the most closely guarded borders in the world''. Ironically it was a Soviet holiday honoring the nation's border guards, who were evidently less than alert.

[Adapted from an article by Carol J. Williams, Associated Press Fri 29 May 1987 and subsequent reports]

Soviet Air Defense Penetration

Eugene Miya <eugene@ames-nas.arpa>
Mon, 1 Jun 87 09:26:11 PDT

Seeing that the Soviets also have a lookdown radar capability and this man flew for hours in Soviet airspace, this makes me wonder more about the limitations of such systems (also in the Stark incident). I have not seen a topographic map of the area he flew in, nor have ideas about traffic patterns in the SU, but I think there are computers and software in this (still probably not a computer problem but a C^2I problem which the Stark incident has resolved into), and it's too bad we don't have Soviet correspondents to flame about this.

--eugene miya

[Apparently the plane was observed at various points along the way, but was flying so SLOWLY that air reconnaissance was difficult! I omitted this item from RISKS-4.92 because it seemed only marginally relevant at the time. The computer part of the Soviet air defense system seems not to have been a problem. However, I become more convinced with each passing RISKS Forum that it is human failings that underly our most interesting RISKS cases -- requirement errors, design flaws, implementation bugs, operational glitches, system misuse, or just plain human screw-ups, whether or not a system is heavily automated. From now on I will no longer work so hard to justify inclusion of human misuses of technology (or human misuses of what should have been done by technology but was not). In this case several heads have rolled -- the Soviet defense minister retired, the air defense commander was fired, and other jobs are considered in jeopardy.

It is interesting to contrast this case with the KAL 007 -- there are similarities and significant differences. There are also some parallels with the Stark episode. ``Who would ever think that a plane approaching Moscow was not properly authorized?!'' PGN]

[With respect to it having been "National Border Guard Day":]

[There's an old Swedish joke that the Norwegians will invade on a summer weekend, when the entire Swedish army is on vacation. Martin Minow]

Exocet, PHALANX, chaff, and missile defense

Sean Malloy <malloy@nprdc.arpa>
Mon, 1 Jun 87 07:27:29 PDT

I've watched the discussion in RISKS about the Exocet, the performance of the PHALANX system, and missile defense, and in a number of cases have wished that less of what I knew was classified, so I could correct mistakes that have been put into comments. There are, however, some details that I can talk about freely.

The Phalanx system installed aboard ships has a theoretical arc of fire of 270 degrees, subject to cutouts from ship structure. The placement of the system aboard the FFG-7 class results in the system retaining most of its theoretical arc of fire. Unfortunately, the design of the FFG-7 precludes installing a second Phalanx - there's no place to put it. However, the lack of a forward firing arc is not serious in most cases, as I will show below.

As the author of the only interactive chaff-launcher training simulator in use by the Navy at this time (at least, according to the information I get from the Fleet Combat Training Center here, where the program is in use), I think I am qualified to comment on the use of chaff as a missile defense.

The effective use of chaff in missile defense depends on several factors - the speed and direction of the relative wind, the specific design of the ship's superstructure, and above all, detecting the missile as soon as possible.

The two basic tactics for decoying a missile with chaff are to 1) give the missile a 'better' target than the ship to track and 2) use the chaff to pull the missile's aim away from the ship after the missile has locked on to the ship. To do this, the chaff must present a larger radar cross section (RCS) than the ship.

All ships have a variable RCS, depending on the angle the ship makes with the missile's course. The smallest RCS occurs with the bow or stern about 15-20 degrees off the line of the missile's course. If the ship is beam-on to the missile, in most cases, all the chaff the ship can fire isn't going to help.

The relative wind is important because, first, the idea is to get the missile to follow the chaff away from the ship, and since the chaff moves at the speed of the relative wind, its movement is dependent on the wind, and second, the chaff launchers don't throw the chaff rounds that far away from the ship - a good relative wind is necessary to give the chaff enough separation to allow it to appear as a separate target for the missile to pick to track instead of the ship.

Finally, the missile must be detected as soon as possible. The chaff rounds aren't immediately effective. It takes time for the round to reach its 'bloom' point, and another second or two for the chaff cloud to bloom. If the missile is close enough, there won't be enough time for the chaff cloud to form at all, or the chaff cloud won't have enough separation to be useful. From the information gathered from the chaff simulation I wrote, you generally need between 30 and 60 seconds of warning to be able to deploy chaff effectively.

The big advantage in the use of chaff, however, is that it's simple and quick to use, if you get the warning. A four-position rotary switch, an ARM button, and six firing buttons for the six rounds in a launcher box comprise the entire console, which is part of the SLQ-32 console. The SLQ-32, the ELINT and ECM equipment, should have been manned while the Stark was in the Gulf. It is the responsibility of the ECM operator to detect the lock-on of the firing aircraft, and to use chaff and other soft-kill measures against an incoming missile. From the information I've seen on the Stark incident, whoever was at the SLQ-32 console has to have been asleep at the switch, and is probably going to get raked over the coals, along with the CO and the OOD.

Sean Malloy, Naval Personnel Research & Development Center,
San Diego, CA, 92152-6800 (VOICE) (619)225-6434
(soon to be malloy@nprdc.mil)

[Thanks for letting us in on what you could.

I noted with interest the articles in this morning's paper, which imply that there were no technological failures, only human failures... Does that sound familiar? PGN]

[Subsequent messages from Sean Malloy]

The paper here this morning says that the CO, the XO, the TAO, and the WCO can all be held culpable. I'm not sure, because I don't know how the watchbill is set up aboard an FFG-7, but I think that the Tactical Action Officer and Weapons Control Officer may be the same person under normal circumstances - there may not be more than one officer on duty in CIC, and the designation of TAO is dependent on who is on duty - all of the command officers should have been through TAO school.

It all goes to show that having fity million dollars worth of technological support doesn't do you any good if you don't use it [properly].

Re: Phalanx Schmalanx [For the record]

<Iglesias%UCIVMSA.BITNET@wiscvm.wisc.edu>
31 MAY 87 20:58-PDT

> Years ago, the US Army had a weapon called the "Chapparal", which
> was a 20mm gatling mounted on an armored personnel carrier....

You may be confusing the Chapparal with something else. The Chapparal had 4 Sidewinder missiles mounted on an armored personnel carrier. My dad worked on it when it was being designed and tested. There was talk at one time of putting some kind of guns on it for self-defense.

Mike Iglesias, University of California, Irvine

Re: Computer thefts (re: RISKS-4.82)

Brian Matthews <cxsea!blm@seismo.CSS.GOV>
1 Jun 87 22:45:03 GMT

I was at a local computer dealer recently. I'm friends with some of the people who work there, so I was in back in the repair shop. Someone had brought in an Apple LaserWriter to be fixed. They had purchased it about six months before, and at that time purchased a security device consisting of a plate with some (allegedly) permanent adhesive, attached to a thick steel cable. Unfortunately, when they installed the device, they placed it in such a position that the steel cable extended over an access door in the bottom of the LaserWriter, making it impossible to repair the machine. But, as anyone good repairperson knows, if something's in the way, you take it off. In about ten seconds, with only a normal slotted screw driver, the "permanent" security device had been removed, leaving only a few scratches

on the bottom of the LaserWriter!

The moral is two-fold: first, be careful when installing any security device, so it can be removed, or isn't in the way for normal use or repair, and second, no security device is perfect, and some are less perfect than others.

Brian L. Matthews Computer X Inc. - a division of Motorola New Enterprises
...{mnetor,uw-beaver!ssc-vax}!cxsea!blm +1 206 251 6811

TRW's Credentials (Alan R. Katz)

Jonathan Handel <jlh%acorn@oak.lcs.mit.edu>
Mon, 1 Jun 87 13:10 EST

I'd like this information too, but I don't think people should have to pay $35 a year for this service. I think that TRW and other credit bureaus ought to be required to send you a notice, for free, whenever your credit record is queried or modified.

At present, we treat databases containing personal information as though they were (almost) equivalent to any other corporate asset belonging to the company that compiles the data base. Existing regulations on data privacy are a moderately weak compromise between commercial interests and privacy rights. I think the balance needs to shift.

-Jonathan

Search RISKS using swish-e

THE RISKS DIGEST

Forum on Risks to the Public in Computers and Related Systems

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

Volume 4: Issue 94

Tuesday, 2 June 1987

Contents

Australian Computer Crime

<DParker@Stripe.SRI.Com>
Tue 2 Jun 87 11:16:51-PDT

A sophisticated computer crime occurred in Australia recently and is being investigated by Kevin Fitzgerald and Stuart Gill in Melbourne for the victim company. Sketchy details, more later. A disgruntled employee modified PC circuit boards. One called "Icepick" attacked ACF-2 on an IBM mainframe. The other called "Big Red" was used in a virus attack.

Donn Parker

PCs and Computer Fraud

Peter G. Neumann <Neumann@CSL.SRI.COM>
Tue 2 Jun 87 17:36:48-PDT

The proliferation of PCs and other computers throughout U.S. businesses has led to larger losses to fraud, according to a recent study. Computer crime is on the rise, says a 54-page report by the Cleveland accounting firm Ernst & Whinney, in part because there are more computers in the United States from which to steal. The increasing use of computers in business has raised the sophistication of users and, at the same time, fed the expanding pool of potential computer criminals, the study notes.

The FBI estimates the average loss from computer theft at $600,000, or about 25 times the average loss from "conventional" crime, the report says. Of the 240 companies surveyed, more than half said they have been a victim of computer fraud, which the report estimates costs U.S. businesses from $3 billion to $5 billion a year.

[From PC Week, vol 4 no 21, 26 May 1987.]

Technological vs. (?) human failure

<nancy%icsd.UCI.EDU@ICSD.UCI.EDU>
Tue, 02 Jun 87 16:14:19 -0700

In Risks 4.93 PGN writes:

> I noted with interest the articles in this morning's paper, which imply that there were no technological failures, only human failures...

It seems like man/machine interface issues are greatly ignored in computer science and software engineering. A current court case has the company that wrote the software for a device that killed two people arguing that the fault was the operator's. In this instance, the software and documentation provided the operator with a command that was dangerous to use without any warning about how and when to use it safely (in fact, it probably should not have been provided at all). Was the operator at fault for acting in a natural, human way or was the designer of the equipment at fault for designing a technological device in a way that could easily lead the human to make a mistake? Can the design of a technological device be judged "correct" without considering the environment in which it will be operated?

We design programming languages so that they are less error-prone and discourage the use of some languages because they are harder to use. Should we not also be responsible for doing this for the other types of software we create? We know that humans can make mistakes and, from psychologists, understand a great deal about their "failure modes." If we can consider hardware failure modes in our designs, why not consider human failure modes? Many of the large firms do employ human factors experts, but not enough is done and people seem much too willing to blame the human instead of the technology that failed to consider the human in its design. I am starting to be leery when I read that the technology did not fail, the operator did.

Nancy Leveson, University of California, Irvine

Risk of Inappropriate Technology to Prevent Password Overwrite

Henry Spencer <decvax!utzoo!henry@ucbvax.Berkeley.EDU>
Sun, 31 May 87 00:00:23 edt

> The particular error cited by Bill Young could not have happened if the
> implementation had been in a language such as PL/I or Ada, where
> over-running the bounds of an array is a required run-time check...

I'm not an Ada aficionado, but my recollection is that every PL/I compiler I've ever seen has a turn-checks-off option, and usually it's the default. The reason is clear: such checks are expensive, particularly with a naive compiler that can't eliminate many of them at compile time, and the overrun condition is rare.

> Such checks are clearly not new technology, since Multics (written in PL/I)
> has been doing such for over 20 years. Nor is the technology new to
> hardware, since the Burroughs B5500-series and MCP (written in Algol) has
> also been checking for a similar period.

The distinguishing feature here is that both Multics and MCP are running on special hardware. The reason that these are relatively unpopular systems, while Unix and C are everywhere, is that the latter will run efficiently on almost anything. As we all know, many people will trade off safety for performance any day. As is less widely appreciated, this is not necessarily a foolish thing to do -- it depends on the application. One negative aspect of having hardware and languages that enforce checking is that you have no control over the tradeoffs.

My personal conjecture, not yet verified by experiment, is that with a cooperative language and a reasonable amount of intelligence in the compiler -- more than most current compilers have, mind you -- something like 90% of the run-time checks could be eliminated at compile time, and about 90% of the remainder could be eliminated by reprogramming that would make the program clearer to the compiler (and incidentally to humans) while leaving efficiency unaffected. The remaining 1% might require a way to tell the compiler "believe me, it's right", but otherwise the need for a run-time check could be made a fatal compile-time error. Result: safety with no efficiency penalty. Trouble is, verifying this conjecture would require building such a smart compiler, a sizable project. Maybe next year...

Henry Spencer @ U of Toronto Zoology {allegra,ihnp4,decvax,pyramid}!utzoo!henry

---

A twist on modems calling people

<smv@necis.NEC.COM>
Tue, 2 Jun 87 13:10:25 EDT

The folks at our main facility just installed a new telephone switch, and made two changes which are not user-transparent. The two changes involve the method used to reach our remote switch, and the method used to dial an international call. If you haven't guessed yet, the old international prefix corresponds to the new method of ringing my extension from the main facility. This would be amusing if it weren't for all the auto-dial facsimile machines trying to phone home to Japan with the old dialing codes. They're not much fun to talk to, and they don't seem to report the fact that the calls aren't getting through.

The moral of this story: Get your Fax straight, before you make changes.

Steve Valentine, NEC Information Systems 289 Great Rd., Acton, MA 01720
smv@necis.nec.com

Risks of Compulsive Computer Use

Steve Thompson <THOMPSON%BROWNVM.BITNET@wiscvm.wisc.edu>
Mon, 01 Jun 87 15:33:25 EDT

I saw a piece on the Cable News Network (U.S. cable television station) last night concerning compulsive gamblers. During the roughly 5 minute story, a theory was presented which held that certain types of people may be more likely to become compulsive gamblers than others. I was doing paperwork as I watched, and so was distracted, but I thought they said something to the effect that those people are especially susceptible to the (physiological? psychological?) disease of gambling in much the same way as alcoholics appear to react (physiologically?) to alcohol abnormally.

I was surprised by the comparison, since alcoholics are reacting to a drug (the alcohol), while gamblers are reacting to a behavior. Is it fair to call the gambling a disease, or "simply" a noxious habit?

Anyhow, my train of thought led to computer use. Certainly there are individuals whose attraction to computers is greater than average, and possibly greater than is healthy. I regretfully admit a period as an undergraduate when I would play computer games as a response to a slow social life, which led to a vicious cycle -- my computer use took time that I could have been using to work on my social life. I broke the pattern, but am left with concerns: Need we worry about compulsive computer users? Need there be a Hackers Anonymous? Should compulsive computer use be considered a disease, or a worthwhile funneling of energy? If a disease, the vast number of computers being introduced into the schools and the workplace without our fully understanding the problem seems to present a potentially large RISK to susceptible individuals.

I'd love feedback on these thoughts, as well as knowledgeable responses. It would probably be wise if flames and responses correcting my knowledge of alcoholism, etc., be directed to me and I'll summarize to RISKS.

Stephen W. Thompson, User Services Specialist, User Services
Brown U., Box P, Providence, RI 02912 USA (401) 863-3619

Perhaps the Bill of Rights you sought?

Bruce Wisentaner <wisen@CCA.CCA.COM>
Tue, 2 Jun 87 12:04:46 EDT

Regarding Eugene's message to RISKS about info-age Bill of Rights: See if you have this book in your friendly neighborhood tech library: "FREEDOM'S EDGE: The Computer Threat To Society" by Milton Wessel (Addison Wesley, 1974). It seems to have the Bill of Rights that you seek in its appendix. I have neither the legal right nor the time to type it in.

Bruce Wisentaner

Error(s) in "Phalanx Schmalanx"

Mike Trout <rpics!brspyr1.BRS.Com!miket@seismo.CSS.GOV>
1 Jun 87 12:19:16 GMT

My earlier posting concerning problems in the Phalanx missle defense system contained some errors. I'm not sure how much, if any, of the article is usuable, but I'm a fanatic about accuracy so I'll point out my mistakes.

In one paragraph, I mentioned a U.S. Army vehicle-based gatling gun called the "Chapparal." That is incorrect. The Chapparal consisted of a number of Sidewinder heat-seeking missles mounted on a vehicle, and did not include a gatling. The Chapparal did indeed die a quiet death, probably due to the short range of the missles. There have been, and still are, various types of ground weapons consisting of gatlings mounted on vehicles. They don't seem to be meeting with enthusiastic popularity. My statement about ground-based gatlings having problems with short range and voracious ammunition consumption is generally accurate.

Actually, since that whole paragraph I wrote about ground-based gatlings has marginal relevance to the Phalanx, I suppose it could be deleted.

Sorry about that. Thanks for your attention. Michael Trout
BRS Information Technologies, 1200 Rt. 7, Latham, N.Y. 12110 (518) 783-1161

Search RISKS using swish-e

Report problems with the web pages to the maintainer

Search RISKS using swish-e

THE RISKS DIGEST

Forum on Risks to the Public in Computers and Related Systems

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

Volume 4: Issue 95

Wednesday, 3 June 1987

Contents

COMPASS '87, of particular interest to the RISKS audience

Stan Rifkin <rifkin@tove.umd.edu>
Wed, 3 Jun 87 17:48:42 EDT

COMPASS '87 will be held in Washington DC the week of 29 June - 3 July 1987 at Georgetown University. COMPASS stands for COMPuter ASSurance and is concerned with software safety and process security.

"Our safety, health, and welfare are increasingly dependent on the safe and correct use of computers. Despite advances in software engineering and system design, it is common to find major bugs and untrustworthy performance in critical computer-controlled systems. Existing approaches to computer assurance need to be refined technically and economically, and brand new approaches need to be explored."

The keynote speaker is Harlan Mills, IBM Fellow. Dr. Mills will speak about his quiet revolution at IBM, his "cleanroom" approach to software

development. Dr. Mills is trying to convince the DoD and NASA not to acquire debugged software, rather to buy only software that didn't have any bugs in the first place! And he is receiving a receptive audience.

The keynote address and formal papers will be given on 30 June and 1 July. The other days include special-interest group meetings and a tutorial (2 July) by Nancy Leveson on software safety. COMPASS is sponsored by the IEEE Washington DC Section, NASA, Computer Sciences Corp., and George Mason University. The Proceedings contain some sure-to-be classic papers: Mills on how to acquire software, Neumann on the N best (or worst) computer risks and the implications, several surveys of trustworthy systems and tools, and lessons learned from the NASA Shuttle disaster and other real-world systems. There are panel sessions on software safety, on the role of high-level programming languages, and on legal implications. In addition, there is a banquet talk by Henry Petroski ("To Engineer is Human: The Role of Failure in Successful Design"), and a luncheon talk by John Shore.

For further information on the program or registration, please contact Al Friend in Washington DC either over the network at friend@nrl-csr.arpa or by telephone at 202/692-7235. Many people are staying the weekend after to enjoy the Fourth of July in the Nation's Capital.

Stan Rifkin, Publications Chairman

> [I hope that in early July RISKS will have some relevant comments on Harlan's talks and other COMPASS topics. (Last year's COMPASS program featured a rousing talk by David Parnas as Keynote Speaker.) PGN]

Re: run-time checks (RISKS DIGEST 4.94)

Jerome H. Saltzer <Saltzer@ATHENA.MIT.EDU>
Wed, 3 Jun 87 13:16:41 EDT

Henry Spencer mentions on the subject of run-time checks,

> The distinguishing feature here is that both Multics and MCP
> are running on special hardware...
> ... many people will trade off safety for performance any day...

That comment was widely accepted as the dominating concern in the 1970's, when people were actively debating whether or not to carry forward the hardware features that were required to support Multics and MCP. At the time, hardware features were still quite expensive. But with 1980's technology available, those concerns somehow look diminished.

With moderately clever implementation, hardware run-time checks can usually be done in parallel with the main stream of computation, so they don't directly impede performance that much. At most they have the indirect effect of using up silicon that might have been invested in performance enhancements. They also use up chip design time, but one would expect that cost to be repaid many times in applications development time savings.

It seems to me that there remain two real barriers to introduction of hardware run-time checks:

1. Developing a conviction that they are a good idea. Those of us who have developed programs on Multics or MCP are easily convinced, but those of us who haven't are in a majority.

2. It is hard to sell a new architecture. Life is more rewarding for people who do improved, compatible implementations of old ones.

Jerry Saltzer

[Jerry has put his finger on one of the stumbling blocks in trying to attain systems with critical requirements for security, reliability, safety, etc. There are obvious incentives to use available hardware, software, programming languages, network facilities, etc., even if atrociously malsuited to the application.
[For you old Don Marquis fans, we have a clear-cut case of Archi(tecture) and Compatibel. PGN]]

Risks of Inappropriate Technology to Prevent Password Overwrites

Michael Robinson <MIKE%UTCVM.BITNET@wiscvm.wisc.edu>
Wed, 03 Jun 87 09:33:50 EDT

A very thorough bounds test could be performed millions of times in the time that it has taken you to read this sentence. The test has done nothing to further the purposes of the program, but it has given you that much more cause to believe that the program is working properly. If something IS wrong, you know that you will know about it before it completely wrecks your program.

Dependability, serviceability, future expansion, and the need for defensive posturing are basic engineering concerns -- whether you're building a footbridge or a computer program. They do nothing for the bridge, but they do help to guarantee that something infinitely more expensive than the bridge, namely a human being or his payroll record, won't fall into the waters below. If you can't be sure of that, then the cost of failure has completely eaten up any cost that you "saved" by not anticipating the possibility.

The computer is the least expensive part of the whole scenario. You can always buy a bigger one. If you "waste" a few milliseconds being very sure that you don't have a problem, then it's time well spent. If and when a problem does crop up, then the defensive code kills two birds with one stone: alerting you to the fact that you have a problem, and giving you a clear(er) picture of exactly when, what, where, and why the problem has occurred.

These are some of the ideas that went into the design of the newer languages. It doesn't take much effort to become proficient in any one of them and it behooves us very much to take advantage of them when we can. Bounds tests, "inefficiencies," and all. It's just plain good sense.

Michael Robinson, Univ. Tennessee at Chattanooga, CECA - 413 Hunter Hall

615 McCallie Avenue, Chattanooga, TN 37403, BellNet: (615) 755-4003

Clarification of PL/I array checking (re: RISKS DIGEST 4.94)

Michael Wagner +49 228 303 245 <WAGNER%DBNGMD21.BITNET@wiscvm.wisc.edu>
Wed, 03 Jun 87 14:45 CET

> > The particular error ... could not have happened in a
> > language such as PL/I ... where over-running the bounds of an
> > array is a required run-time check...

I winced when I read this, because 'required' is such an ambiguous word (on whom is the requirement placed), but assumed that people would know enough PL/I to understand. Then came Henry's comment ...

> ... my recollection is that every PL/I compiler I've ever seen
> has a turn-checks-off option, and usually it's the default.

I have experience with only 3 PL/I compilers. Subscript checking defaults to on for two of them (PL/C from Cornell and PL/I Checkout from IBM), and to off for one (PL/I Optimizer from IBM).

> The reason is clear: such checks are expensive, particularly
> with a naive compiler that can't eliminate many of them at
> compile time, and the overrun condition is rare.

We may disagree about what 'expensive' means, but I have examined the output from the PL/I Optimizer with full subscript checking turned on and estimated the cost of run-time subscript checking to be less than a few percent of the total. I ran a production subsystem with checking on for a few weeks, and this yielded a number in concert with my estimates. In the end, I turned subscript checking off, but if the output of the system had mattered in any real sense, I would have considered it false economy.

Michael

Risks for computer junkies

Robert Hartman <sun!rdh@seismo.CSS.GOV>
3 Jun 87 22:38:28 GMT

Regarding Steve Thompson's article about gambling addicts (RISKS-4.94), the drug involved is ... adrenalin! This may also be true for computer junkies. There is indeed cause for worry about the dangers of addiction to a "response-pattern generator" that seems to be so emotionally neutral (giving no feedback whatsoever about the user's habits or characteristics), and as intellectually absorbing as the computer's user interface. (Although the shell isn't the most exciting person to spend time with, it never calls you a jerk either.)

An emotionally vulnerable person can indeed be sucked in, and can tend to lose sight of the fact that dealing with people isn't as straightforward as

dealing with computers. One cannot usually "correct a relationship malfunction" with an "abort/restart sequence" and "different inputs." Because the addict may feel incompetent to deal with people anyway, spending increasing amounts of time on the machine tends to compound his feeling of isolation. This can lead to a vicious circle in which he returns to the relatively "safe" (if emotionally stultifying) environment of the computer, after increasingly disappointing experiences with people that he is less and less able to cope with.

As interfaces get better, this risk gets worse.

-bob. Sun Microsystems, Mt. View

Re: When Computers Ruled the Earth (Bank Stupidity)

Tue, 2 Jun 87 20:56:49 EDT

The ultimate case of bank stupidity came when we bought our house eleven years ago. At that time, they offered us the option of an automatic payment plan, where we gave them the authorization to write a check on our checking account (at a different bank, we're not stupid) for the monthly mortgage payment. As a side bonus, they were willing to do it twice a month for half-payments, which was convenient as I was getting payed twice monthly at the time (not to mention the postage savings).

About a week after we signed all the papers, I got a call from the nice lady at the bank saying that could not put us on the automatic payment plan. The reason? Our monthly payment amount was odd, and the two half-payments had to be equal. A few minutes on the phone and the nice lady checking with her supervisor determined that we were allowed to make a greater payment with the extra money going toward the loan principal, so we increased the monthly payment amount by $0.01 to make the two half-payments equal. And so we thought we had it licked.

Act III: Bank statement arrived at end of month. Two automatic payment checks to mortgage had cleared, each for $0.01!!!

Ed Sachs, AT&T Bell Laboratories, Naperville, IL, ihnp4!ihlpa!essachs

---

Clarification on CHAPPARAL and VULCAN [but for the record]

Bill Gunshannon <bill@westpt.usma.edu>
3 Jun 87 15:30:31 GMT

>From: Iglesias%UCIVMSA.BITNET@wiscvm.wisc.edu
>To: RISKS@CSL.SRI.COM
>Subject: Re: Phalanx Schmalanx [For the record]
>
> > Years ago, the US Army had a weapon called the "Chapparal", which
> > was a 20mm gatling mounted on an armored personnel carrier....
>
>You may be confusing the Chapparal with something else...

The weapon they are trying to identify was called the VULCAN. It was a sister to the CHAPPARAL and was used to shoot down low-altitude aircraft. I served in Europe with 2/60th ADA C/V which was one of the first CHAPPARAL/VULCAN units to be deployed over there. They were the last thing the enemy had to get past before hitting something important like an airbase or equipment depot. That's assuming they made it past the NIKE and HAWK batteries. I believe from what I have seen in the news photos that the PHALANX is merely a sea-going VULCAN.

bill gunshannon

UUCP: {philabs,phri}!westpt!bill PHONE: (914)446-7747
Martin Marietta Data Systems, USMA, Bldg 600, Room 26, West Point, NY 10996

Search RISKS using swish-e

THE RISKS DIGEST

Forum on Risks to the Public in Computers and Related Systems

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

Volume 4: Issue 96

Saturday, 6 June 1987

Contents

Lightning Strikes Twice At NASA

Matthew P Wiener <weemba@brahms.Berkeley.EDU>
Sat, 6 Jun 87 04:22:40 PDT

The 22 May 87 issue of _Science_, p903, has an article about the rocket that was hit by lightning two months ago:

> Jon Busse, chairman of NASA's inquiry into the accident, disclosed ... that the Atlas-Centaur ... was launched in a heavily charged electrical atmosphere on 26 March. The rocket itself triggered a lightning bolt. A single bolt punched through the fiberglass nose cone, spread fingers of electricity around the computerized brain [sic!] that commands the motors,

> and changed one word of program language. As a result, the motors sent the rocket veering off course 51 seconds after lift-off, at the moment of peak strain. The $160-million package began to break up, and flight controllers had no choice but to deliver the coup de grace.
> ... If [shuttle launch criteria] had been applied, they would have prevented the launch of the unmanned Atlas-Centaur this spring. According to one researcher, NASA has installed the ``most sophisticated lightning monitoring system in the world''.... But its data were not used.
> ... There was a failure of communication, Busse said, and a failure of NASA to ``exercise awareness, judgment, and leadership.''

I find it interesting how this example is doubly appropriate for RISKS.
We have both an accidental computer failure, and of the larger human failure to match existing data with actual procedures.

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

Iraqi cockpit navigation system placed Stark in exclusion zone?

Jon Jacky <jon@june.cs.washington.edu>
Thu, 04 Jun 87 21:45:29 PDT

The SEATTLE TIMES, Thurs June 4, 1987, p. A4 includes a story titled "Seconds to react, Pentagon report on Stark says," attributed to The Washington Post and Newhouse News Service. It includes the statements:

"Iraq has claimed that the Stark was inside the "exclusion zone" of the (Persian) Gulf where Iraq had warned ships would be subject to attack, the Pentagon said. The U.S. government disputes the claim.

The Iraqis base their claim on the navigation system in the fighter-plane cockpit, according to the Pentagon, which added "we are convinced Stark was 10 to 15 nautical miles outside" that zone. The Pentagon said it had received a "wealth of position data" on the Stark from that ship, the AWACS plane that monitored the attack and two other ships in the area."

- Jon Jacky, University of Washington

> [It does little good after an autombile wreck to argue that your late spouse had the right of way. Unfortunately, this case is similar. Whether or not the Iraqi navigation system was in error, there were quite a few human lapses that rendered technology useless. PGN]

Run-time checks

<sturgis.pa@Xerox.COM>
Thu, 4 Jun 87 11:13:00 PDT

Most of us in the Computer Science Laboratory at the Xerox Palo Alto Research Center have been using the programming language "Cedar" for several years. Cedar has a "safe" subset which guarantees the "safe" behavior of

compiled programs. One has to use keywords like "LOOPHOLE" or "TRUSTED" in order to program outside the safe subset. Unsafe behavior includes references outside the bounds of an array. Programming in the safe subset causes the automatic insertion of run-time bounds checks, among other run time checks. (It also involves extensive compile time checking as well.)

In our workstation operating system, also called "Cedar", all programs run in a common multi-process address space. This includes programs that are being debugged, as well as editors and the file system. The operating system itself is written in Cedar, and a large part of that system is written in the safe subset. (Some old parts of the system have not been converted to safe Cedar. It is a matter of controversy how much could be converted.) The screen managers, editors, compilers, and mail program are all mostly in the safe subset. Thus, my day to day work is conducted using programs that involve extensive run-time checking.

I rarely have a "crash" on my workstation that can be traced to a failure that could have been caught by a run-time check, such as a bounds check. That is, crashes in which the language abstraction is violated. "Rarely" means on the order of significant fractions of a year between occurrences, probably more than a year. I do have more frequent crashes than this. There are a few resources in our system that are consumed in a monotonic fashion, and under certain conditions one can run out of these resources during a day of work; this event requires a re-boot. In addition, there are some lingering deadlocks in the window manager that strike infrequently.

I have recently written a large compiler-compiler system. Except for a few lines of code in the midst of a parser generator subsytem, it is written entirely in the safe subset. This system generates Cedar source code, and generates this source code faster than the Cedar compiler can compile it. Thus, the cost of the run-time checks in this program is inconsequential. I debugged this system on my workstation, running it concurrently with may day-to-day support tools, including the window manager, text editor, compiler, and mail-program. This undebugged code never interfered with the execution of these support tools.

All of the above is written to support the notion that one can work on a day-to-day basis in a system with extensive built in run-time checks. I find it very comforting to work in this system. I personally would find it very painful to go back to a world that was not "safe".

Howard Sturgis

Run-time checks

<decvax!utzoo!henry@ucbvax.Berkeley.EDU>
Sat, 6 Jun 87 02:54:42 edt

I should clarify a couple of points in my previous contribution. Several people have pointed out IBM's internal PL.8 compiler, which does generally resemble what I was thinking of: it works quite hard to determine whether run-time checks are really needed, and succeeds in eliminating most of them.

It typically manages to bring the run-time-check overhead down to one or two percent, sometimes to zero. (PL.8 has not been publicized much, but there are a couple of papers on it in the Sigplan 82 compiler symposium.)

My notion was a little different, though: the compiler should *never* generate a run-time check; if a run-time check is necessary anywhere, and the programmer has not explicitly overridden that particular check in that particular place, this should be considered a fatal error and code generation should be abandoned.

The reasons behind this are two. First, the occurrence of a run-time error is almost certainly a symptom of a bug; programs should be more careful. It seems better to flag such bugs at compile time, when it is convenient to do something about them. Second, since the actual error will generally show up at some remove from the underlying bug that caused it, it is really very difficult to do anything intelligent about it after the fact, barring global recovery methods like recovery blocks. (This is a major reason why programs should avoid generating such errors.) Dying with a core dump is not acceptable for e.g. an air-traffic-control program. It seems wise to head off such errors in advance.

Clearly, it is not realistic to expect a compiler to eliminate all run-time checks from arbitrarily complex programs. That's more a job for a theorem prover, which isn't practical as a routine programming tool for normal applications just yet. But: programmers do not write arbitrary programs. My conjecture -- which PL.8 strengthens but does not prove -- is that modest intelligence in the compiler, plus some willingness to clean up code to make it clearer, would reduce the "compiler can't be sure about this one" cases to an occasional annoyance that could be handled by manual overrides.

Henry Spencer @ U of Toronto Zoology
{allegra,ihnp4,decvax,pyramid}!utzoo!henry

Some experience with run-time checking

<James_M._Bodwin@um.cc.umich.edu>
Thu, 4 Jun 87 15:49:24 EDT

I'm the author of a Pascal compiler that is compatible with the IBM Pascal/VS compiler. Among other things, the compiler does a MUCH more complete job of detecting run-time errors than the IBM product does. For instance, my compiler detects run-time uses of variables before they have been assigned to or otherwise initialized. Since the compiler is completely compatible with the IBM product, one of the first things that people did when the compiler was released was to dust off existing Pascal/VS programs and run them through the new compiler. The number of bugs that the new compiler found in these supposedly "fully debugged" programs was absolutely frightening. I now regret that I did not have the foresight to keep statistics on this since it would have given some kind of indication of the effectiveness of the particular debugging techniques used. Even more frightening was the number of programmers who refused to believe that this new compiler had actually found errors in production programs. I've often

thought that it would be an interesting experiment to have a group of programmers debug some programs with all compiler run-time checking off and then to turn the run-time checking on in order to see how many errors they missed.

One risk of putting strong run-time checking into a compiler is that the programmers may assume that the compiler is doing more than it is. For instance, the IBM Pascal/VS compiler does not detect integer overflows in EVERY circumstance (it isn't clear if this is a "bug" or a "feature"). Thus, a few programmers were really surprised when the new compiler detected integer overflows in their programs. They had not bothered to test for that themselves since they were convinced that the Pascal/VS compiler was doing the checking for them.

Jim Bodwin

Bounds checking

Alan Wexelblat <wex@MCC.COM>
Thu, 4 Jun 87 12:37:04 CDT

There's a risk associated with hardware bounds checking which continues to nab me. After working for months on Burroughs hardware (in Modula2 and ALGOL) I became accustomed to having my occasional bounds errors caught by the compiler or the hardware. Now I work in C on a UNIX box and occasionally am astonished when the first element of an array "miraculously" takes on a new value. Makes debugging a lot harder, too.

Alan Wexelblat
UUCP: {seismo, harvard, gatech, pyramid, &c.}!sally!im4u!milano!wex

---

Error Checking and Norton's Assembly Language Book

"James H. Coombs" <JAZBO%BROWNVM.BITNET@wiscvm.wisc.edu>
Thu, 04 Jun 87 13:07:40 EDT

While working through *Peter Norton's Assembly Language Book for the IBM PC*, I was struck again and again by it's "risky" approach to programming. A few quotations:

On error checking:

> In this first version of READ_SECTOR we'll deliberately ignore errors, such as having no disk in the disk drive. This is not good practice, but this isn't the final version of READ_SECTOR. We won't be able to cover error-handling in this book, but you will find error-handling procedures in the version of Dskpatch on the disk that is available for this book (169).

At another point that I could not locate just now, they (Norton and Socha) say that they will not check for X, since it is a programming error.

One could interpret the ignoring of error-checking in a number of ways---perhaps it is so important that the reader should spend $24.95 (for the diskette) to get some good examples; perhaps the authors are bored by it; perhaps it would make the book too large; etc. In any case, the book does not make an effort to impress upon readers the importance of extensive and careful error checking. Since they attempt to teach modular programming at basic levels, it would be appropriate for them to teach error checking at basic levels as well. They do stress the importance of TESTING, especially boundary conditions, but they clearly believe that testing can replace most error checking.

On completeness of programs:

> Dskpatch won't be finished then, as we said, programs never are; but the scope of our coverage in this book will be complete (280).
>
> "a program is never done . . . but there comes a time when it has to be shipped to users" (295; quotation marks are in the book, apparently to indicate that this is conventional wisdom).
>
> Remember: Programs are never complete, but we have to stop somewhere (276; and then they kludge a routine that they admit should be completely rewritten).

This attitude explains why the book gradually gets sloppier and sloppier. The first few chapters impressed me as award-winning material, wonderful tutorial, careful, thoughtful.... Then I found that care replaced more and more by an effort to sell the diskette and by haste to finish the book and get more dollars in their pockets. In some ways, I appreciate the errors that I found in their programs, since that gave me a chance to try out my knowledge of assembly language, but that does not excuse their attitude and certainly does not excuse their teaching others to meet deadlines by handing programs over as is instead of completed.

I would still recommend this book for experienced programmers who want a good tutorial on assembly language, but it would be a little dangerous for people who have not already absorbed some of the principles of risk reduction.

In addition to this example of risky programming, I would like to offer some thoughts on the discussion of such built-in error checking as checking for the overflowing of array bounds.

First, aren't the gains fairly limited? If the error is captured in the hardware, it's still going to cause an abort, right? It may be a little cleaner and may help the programmer locate the problem, but the program is still going to crash. I certainly wouldn't want the hardware or even any compiler-generated code to attempt to correct such an error in my code. I suppose that there may be some disagreement about the gains of terminating gracefully over just falling apart, but the point is that one still has to terminate, which is not much consolation to the user. If the error condition could cause damage to the system, then the gains might be considerable. Such damage is usually prevented at the systems level though. On an IBM mainframe, one has such things as "operation exceptions." What about other machines?

In three years of program development, I have yet to damage an IBM PC. In "critical" software---well, maybe there is something here---would built-in boundary checking prevent a robot from smashing someone's head? From the user's point of view, that certainly would be consolation!

Second, what is the overhead for such checking? In an inner loop, the overhead might be substantial, especially if the loop consists of only a few lines, as in searching for a character in a string. The programmer has to code some termination anyway, so error checking should be redundant here. E.g.,

```
for (i = 0; i < BUFSIZE && buf[i]!=CHAR_X; i++);
```

I suppose the programmer could slip and use BUFSIZE when it should be BUFSIZE2 or something like that. (For a real example of such an error in distributed code, see the public domain version of SED, "a freeware component of the GNU operating system"---in the incarnation in which I received it from a BBS, same version on Genie, I believe.)

Finally, checking for array bounds is of little value in languages/programs that use pointers extensively. The loop above is much more likely to be coded as follows:

```
for (s = buffer; *s && *s!=CHAR_X; s++);
```

A superb compiler might be able to determine that this is an appropriate point to check for going past the bounds of 'buffer', which may not be properly terminated. By such standards, however, today's compilers are Neanderthals, and most of our machines don't have the power to drive more intelligent compilers at reasonable speeds anyway.

In conclusion, I don't believe that built-in error checking is worth the trouble for most environments. First, the gains are limited. Second, the overhead may be substantial and cannot be controlled by the programmer. Finally, compilers are not capable of interpreting the code well enough to determine just what sort of error checking should be performed (perhaps I should say compilers that I am familiar with on equipment that I am familiar with: PL/I on IBM mainframes; C86 and MSC on IBM PCs).

James H. Coombs, Mellon Postdoctoral Fellow in English, Brown University

---

Re: Risks of Compulsive Computer Use

Douglas Jones <jones%cs.uiowa.edu@RELAY.CS.NET>
Thu, 4 Jun 87 10:29:25 CDT

Steve Thompson wrote (Risks 4.94) "Need there be a Hackers-Anonymous."

In 1972 or 73, while I was an undergraduate at Carnegie-Mellon, I made up a supply of flyers for 'Computer Nurds Anonymous' and posted them around campus. (Note: Nurd was the accepted spelling at CMU back then; we had not picked up on the MIT spelling, nor was the word 'hacker' used much at

CMU at the time.) Computer Nurds Anonymous offered a withdrawal plan that moved the nurd from interactive computing to a batch environment, and from there, in graduated steps, to hand cyphering. I understand that some copies of the flyer ended up at other universities; I no longer have a copy.

More seriously, while I was an undergraduate, I and another student did a term project for a personality theory course which involved what may well be one of the first serious psychological studies of hackers. We came up with the following characterization:

> This particular group of students uses the computer as a social surrogate and as an object of their creative energies because, being passive individuals, they prefer to deal with the stable environment of the machine world. As these people are basically intelligent but introverted, they employ the computer because it is intellectually stimulating without allowing the trauma of social contact.

We then identified a group of 28 students who had completed some course work in computer science, 6 of whom were identified by their peers as 'computer nurds'. We administered the Edwards Personal Preference Scales for change (Do they like familiar environments, or do they seek new environments?) and order (Do they like an orderly life?), and the Minnesota Multiphasic Personality Inventory social introversion scale. We found no correlation between being a 'computer nurd' and desire for change, we found that, as expected, 'computer nurds' were more likely to be introverted than extroverted, but that this was true of the entire population tested also. We found, contrary to our expectations, that 'computer nurds' were significantly more disorderly than others.

Charles Hedrick (who was then a PhD student at CMU) commented on our unexpected result on disorder that, while an orderly disposition was logically a prerequisite for a successful programmer, so-called 'computer nurds' are not terribly successful. Nurds spend a great deal of time at the computer, but they operate it more as a toy than a learning tool; they are adept at performing tricks with a teletype but lack the orderliness required for true success.

Douglas W. Jones

A reference on Information Overload; a Paradox of Software

<eugene@ames-nas.arpa>
04 Jun 87 11:13:28 PDT (Thu)

%A Spectrum Staff
%T Too Much, Too Soon: Information Overload
%J IEEE Spectrum
%V 24
%N 6
%D June 1987

%P 51-55
%K IFF, human factors

Jerry Saltzer's comment: Ah, that's my "Paradox of Software" argument. We want it fast (who would use a computer slower than a person?), yet we want it flexible, friendly and maintainable when it breaks down. I wish I were doing more research in software, but I am surrounded by people who only want the computation done faster, almost at all costs. E.g., would we prefer a single button on ALL keyboards which reads "HELP" (single button, very fast), or a more general, flexible keyboard which has 'H' 'E' 'L' 'P'?
--eugene miya

Computerholics

"James H. Coombs" <JAZBO%BROWNVM.BITNET@wiscvm.wisc.edu>
Thu, 04 Jun 87 14:01:26 EDT

Steve Thompson asks about people addicted to computing. So far as I know, we don't have a definition of addiction; we have, at best, some criteria for determining when a person is addicted. In fact, I believe that we have levels of addiction. For example, we have "problem drinkers," and we have "alcoholics." Do we also have "problem computors" and "compuholics"?

First, I think we need a careful characterization of addiction, with respect to computing. Until we have that characterization, I don't think we can profitably address Steve's questions.

Just to start things off, I suggest that a person P is addicted to an activity A (which may include the taking of substances) iff (if and only if):

1) A is being engaged in to an extent that is physically and/or mentally debilitating.

2) A is such that the benefits of not engaging in it outweigh the benefits of engaging in it.

3) P cannot cease A.

Clause (1) is necessary to exclude such necessary activites as eating. Clause (2) is necessary to account for such things as living, which is progressively debilitating; presumably, we don't want to say that people are addicted to living (and don't want to get into discussions of when people would be better off dead?).

I'm not sure, but it seems in some ways right to add a clause specifying that P knows (1 and 2) or even (1, 2, and 3). I hesitate to add this though, because it also seems right to say that a person can be addicted to something without having any idea that there is a problem. This consideration threatens to bring up issues of social definitions, relativism, and all of that; but let's not.

So, a preliminary result given this definition. The benefits of being addicted to computing instead of to other activities are trivial, since the addiction

leads to physical and/or mental disability. Note that under certain circumstances, the disability may be justified, but this is covered by clause (2). In a state of emergency, it may be appropriate to exploit the addict's computing abilities, just as it may be appropriate to ask the police to stop a killer in a shopping mall. ON THE OTHER HAND, if a person is so addictive that he/she must be addicted to SOMETHING, then it would certainly be better to be addicted to computing than to some more damaging activity (such as drinking alcohol), and this is covered by clause (2).

Theoretically, I think this definition takes us a long way. Practically, it doesn't seem to offer us much. How are we to determine whether or not, for example, a person is so addictive that he/she must be addicted to something? Are we to beat on that person until we teach him/her to live with no addictions? Or is it better to let up at some point and say "this is good enough." Also, we have the problem of levels of addiction, and this is not addressed in the definition. If one is computing at a level that is only problematic, then is that better than being fully addicted to something that is less dangerous than the computing?

Also, I see that I said in (3) that P CANNOT cease A. But, don't addicts often (with extensive help) cease their addictive activities? Perhaps we should say in (3) that P cannot cease A on his/her own. Then we might define a person who has a problem with A as someone who can cease A on his/her own but is having difficulty doing so.

Then, it seems that we have to say that being problematic with respect to A is better than being addicted with respect to A' iff the costs of the full span of engaging in A are less than the costs of the full span of engaging in A' (add after effects to each). If being a problematic drinker ruins your liver, why not be a computing addict instead? But if addictive computing ruins your eyes and causes skin cancer, but your liver problem is limited to a few spots, why not damage the liver a little? If addictive computing ruins your health over a twenty-year period but being more of a participant in normal social activities would have infected you with AIDS, why not compute yourself into the grave?

Finally, I would like to encourage people to quit worrying about other people being isolated. Whenever someone doesn't want to join the circle, people have to figure out what his/her problem is. To say that the person is addicted to computing (or to work) seems like an au courant easy answer. Some people haven't an inkling of what happens in isolation, and many people seem to know little more than herd instinct and the word "normal" (not the concept, just the word). To these people, isolation seems physically and/or mentally debilitating. It would be much better if people would accept others a little more and give them credit for knowing their best interests instead of addressing their own doubts by stigmatizing what they don't understand.

Ceteris paribus, then, I think we should drop "isolation" from our concerns about the risks of computing. There is nothing absolutely bad about isolation, and some people can gain a lot by a week or so of solitude. Of course, prophets tend to go off for much longer than a week; forty days and forty nights seems like a good healthy period for a prophet. I think we should allow at least that to computer gurus, even if their activities are less grand.

James H. Coombs Mellon Postdoctoral Fellow in English Brown University

Naval Warfare -- on possible non-detonation of missiles

Mike McLaughlin <mikemcl@nrl-csr.arpa>
Thu, 4 Jun 87 11:34:50 edt

In WWII, a Japanese battleship with HUGE (17" or 18") guns hit a U.S. destroyer with very nearly a full salvo... of armor piercing projectiles. The range was close, and the trajectory of the projectiles was close to the horizontal. The projectiles passed completely through the target, without detonating - the destroyer was simply not there, as far as the fuzes were concerned. The U.S. ship took a fair amount of injuries and damage, but was still able to sail on its own power back to a friendly port. Just a couple of the projectiles exited below the waterline, and the crew was able to control the flooding and fire.

PT boats, on the other hand, were sometimes destroyed by the water spouts of major caliber projectiles.

Not much relation to today's Risks in Computing - except for a little perspective on the history of projectiles against ships. Projectiles are just ballistic missiles without on-board guidance. The larger projectiles have fuzes that used to be set mechanically just before firing. If you don't have time to set them right, they do not do what is desired. Sounds like human error again... or perhaps, before.

- Mike McLaughlin <mikemcl@nrl-csr.arpa>