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 2

Saturday, 31 May 1986

- Overload of a different sort [Air traffic stoppage] (Ted Lee)
- Cordless Phones Cry Wolf! (Peter G. Neumann)
- The Mob Breaks into the Information Age (Mike McLaughlin)
- [Non]computerized train wreck (Mark Brader)
- Ballot Integrity; Specialization in Decision-Making (Tom Benson)
- Network Security, Integrity, and "Importance" (Kurt F. Sauer)
- Modems (James R. McGowan)

Issue 28 (17 Mar 86)

- Risks of commission vs. risks of omission (Dave Parnas and Peter G. Neumann)
- The TIME is RIPE -- a clock problem (Peter Neumann)
- Mailer Gone Mad? (Landrum)
- Money Talks (Matthew Kruk)
- Another discourteous modem (Glenn Hyatt)
- Will the modem discussions ever hang up? (Rob Austein)

Issue 29 (17 Mar 86)

- Commission vs. Omission (Martin J. Moore plus an example from Dave Parnas)
- A Stitch in Time (Jagan Jagannathan)
- Clockenspiel (Jim Horning)
- Cordless phones (Chris Koenigsberg)
- Money talks (Dirk Grunwald, date correction from Matthew Kruk)
- [Non]computerized train wreck (Mark Brader)
- On-line Safety Database (Ken Dymond)

Issue 30 (18 Mar 86)

- Classes of Errors (Scott Rose)
- Range Safety System (David desJardins)
- Commission vs omission (Geoffrey A. Landis)
- Stupid Clock Software (Dave Curry)
- Control characters in headers from eglin-vax (Martin J. Moore)
- Money Talks (Prasanna G. Mulgaonkar)

Issue 31 (19 Mar 86)

- Still more on shuttle destruct systems (Martin J. Moore)
- Clock Synchronization (Andy Mondore)
- Timestamp integrity at system startup (John Coughlin)
- Danny Cohen on SDI (Charlie Crummer)
- Two more mailer problems (Sidney Markowitz)
- Marking money for the blind (Atrocity Joelll)
- Why would anyone want to computerize voting? (Larry Campbell)

Issue 32 (20 Mar 86)

- Om/Comm-ission, and analysis of risks (Niall Mansfield)
- RSO's and IIP's (Dave Curry)
- Complex systems ru(i|n)ning our cities (Mike Mc Namara)
- Re: Two more mailer problems (Bernard S. Greenberg)
- Banknotes for the visually handicapped (Nigel Roberts, Barbara E. Rice)
- Psychological and sociological consequences (Harald Baerenreiter)

Issue 33 (23 Mar 86)

Computer Naivete (Lindsay F. Marshall)
- Admissability of computer files as evidence (Scott E. Preece)
- Programming productivity (Henry Spencer)
- The San Jose Public Library [and responsibilities] (Sriram Vajapeyam)

● Issue 42 (14 Apr 86)

- Robot safety (Ron Cain via Bill Park)
- Use of computer files as evidence (Rob Horn)
- Review of *Softwar* (Gary Chapman)
- Computerized Voting -- No Standards and a Lot of Questions (Summary of Eva Waskell's talk by Ron Newman)

● Issue 43 (17 Apr 86)

- Re: Review of *Softwar* (Marvin Schaefer)
- GREAT BREAKTHROUGHS (Herb Lin)
- Star Wars software advance (AP)
- Smart bombs in Libya (Washington Post)
- Pacific Bell Bills (SF Chronicle)
- BU joins the InterNet... (Barry Shein)

● Issue 44 (21 Apr 86)

- Why Simulation Is A Good Thing... (Lynne C. Moore)
- Hacking & forgery laws (Robert Stroud)
- Strategic Systems Reliability Testing (Dan Ball)
- SDI (Larry Campbell)
- Cost of phone billing error (Dave Redell)
- Normal Accidents and battle software (Dave Benson)
- Psychological risks, part II (Dave Benson)

● Issue 45 (28 Apr 86)

- HBO gets Hacked:: We Interrupt This Program ... for a Viewer Protest. (Geoff Goodfellow, Frank J. Wancho)
- Ball's contribution on Polaris and SDI (from Dave Parnas)
- SDI Reliability Testing - Offensive deterrent vs SDI (Jon Jacky)
- What are the limits to simulation? (Eugene Miya)
- Reference on admissibility of computer records (Bill Cox)
- Phone billing error at Pacific Bell, etc. (John Coughlin)
- Cracked Libya Defense (Udo Voges)
- Challenger article (Ron Minnich)

● Issue 46 (29 Apr 86)

- Martin J. Moore (on Challenger article)
- TV "piracy" (Nicholas Spies)
- HBO -- Hacked Briefly Overnight (Mike McLaughlin)
- The dangers of assuming too much -- on TMI-2 (J. Paul Holbrook)
- A POST Script on Nuclear Power (Peter G. Neumann)

● Issue 47 (1 May 86)

- HBO hacking (Phil R. Karn, Dan Franklin)
- What are the limits to simulation? (Herb Lin)
- Strategic Systems Reliability Testing (Herb Lin)
- Correction on Challenge Discussion (Jeff Siegal)

- Issue 55 (28 May 86)
  - Culling through RISKS headers; SDI (Jim Horning)
  - Blind Faith in Technology, and Caspar Weinberger (Herb Lin)
  - Risks of doing software quality assurance too diligently (PGN from Chris Shaw and the Torrance Daily Breeze)
  - Collegiate jungle (Mike McLaughlin)
  - Decease and Desist -- Death by Computer (Deborah L. Estrin)
  - The Death of the Gossamer Time Traveler (Peter G. Neumann)
  - Computer Ethics (Bruce A. Sesnovich)
- Issue 56 (30 May 86)
  - A joke that went wrong (Brian Randell)
  - Computer Program for nuclear reactor accidents (Gary Chapman)
  - On risks and knowledge (Alan Wexelblat) [Excerpt]
  - Technical vs. Political in SDI (Dave Benson)
  - Are SDI Software predictions biased by old tactical software? (Bob Estell)
  - Culling through RISKS headers (Jim Horning)

Search RISKS using swish-e

Report problems with the web pages to the maintainer

THE RISKS DIGEST

Forum On Risks To The Public In Computers And Related Systems

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

Search RISKS using swish-e

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

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

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

Feeds

RSS 1.0 (full text)

RSS 2.0 (full text)

ATOM (full text)

RDF feed

WAP (latest issue)

Simplified (latest issue)

Smartphone (latest issue)
Under Development!!

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

Please 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 2: Issue 1

Saturday, 1 Feb 1986

Contents

First Six Months of the Forum in Retrospect; Updated Disaster List

Peter G. Neumann <Neumann@SRI-CSL.ARPA>
Sat 1 Feb 86 00:18:03-PST

With RISKS-1.45, my MM saturated completely on its ability to cope with all of the Volume 1 issues of the RISKS Forum (at 289 pages) in one .TXT file, so it must be time to start Volume 2! Thus, let me take this opportunity to review the six months since RISKS Volume 1 Issue 1, on 1 August 1985.

The SDI pallaver seems to have overwhelmed some of you, but it has opened up some serious problems -- as does the unreleased Eastport Report, which is perhaps most interesting for what it does not cover! (You may have concluded that SDI is a religious issue that cannot be decided rationally?) The Space Shuttle tragedy also opens up all sorts of questions on how much trust we can place in technology and what the risks are -- although those questions have been around all along. They are simply elevated to a higher level of public awareness now (temporarily?). For example, the issue of the safety of self-destruct mechanisms has been lurking, and is clearly a concern in general -- but is only one concern. There are lots of others. We must remember that risks come many sources -- not just from maliciousness and accidents, but also from unforeseen combinations of problems.

So far we have addressed many important issues, although some of them quite superficially. We have overlapped on occasions with ARMS-D, Soft-Eng, and Security distributions. However, it seems that RISKS does provide a focus that cuts across these other mailings, and that it serves a useful purpose -- particularly when it indeed focuses on the risks to the public.

A few platitudes are in order:

No system is ever going to be 100% guaranteed all of the time, especially if it runs standalone. Even with humans in the loop, humans can make mistakes -- especially in real-time.

Risks may come from unexpected directions. A system that has run perfectly may still suddenly malfunction. Hardware may fail. Bugs may remain undetected for years, and suddenly become activated. Besides, software may age poorly, especially if changes somewhere else interfere with old working software.

The operating environment may contain risks that undermine sound design, impementation, and operations.

The notion that all critical concerns -- security, reliability, etc. -- can be confined to a small portion of a computer system or distributed system (e.g., a kernel) is a fantasy, particularly with conventionally designed systems.

The notion that distributed control solves problems that cannot easily be solved with central control is also often a myth -- problems of updating, synchronization, concurrency, backup, verifiability, etc., may be equally severe in many operating environments.

Lowest-bidder efforts are intrinsically risky. Commercial software is commonly far behind the state of the art. That may be an advantage in some cases (!), but is often detrimental. But there are significant benefits to be gained from using certain software engineering techniques.

There are inherent risks in using computer systems in critical environments. These must be continually reexamined. Critical and open discussion of critical systems and critical environments is essential. We as technologists must better understand the risks and their implications. And we must apply that increased understanding to new developments.

And now, a word from our sponsor: This forum was established at the request of the Association for Computing Machinery, and chartered as an activity of the ACM Committee on Computers and Public Policy (of which I am the chairman). However, the opinions reflected herein do not constitute an endorsement by the ACM. On the other hand, if I screw up and do something the ACM does not like, I probably lose my (volunteer) job.

As a summary of some of the problems that have occurred, and as a possible inspiration for undiscussed areas of concern or areas of hope, I include in this issue an update of the disaster list that those of you who have been with us since the beginning saw in Vol 1 No 1.

Peter

****

SOME COMPUTER-RELATED DISASTERS AND OTHER EGREGIOUS HORRORS
Compiled by Peter G. Neumann (31 January 1986)

The following list is drawn largely from back issues of ACM SIGSOFT Software

Engineering Notes [SEN], references to which are cited as (SEN vol no), where
vol 11 = 1986. Some incidents are well documented, others need further study.
Please send corrections/additions+refs to PGNeumann, SRI International, BN168,
Menlo Park CA 94025, phone 415-859-2375, Neumann@SRI-CSL.ARPA.

Legend: ! = Loss of Life; * = Potentially Life-Critical;
    $ = Loss of Money/Equipment; S = Security/Privacy/Integrity Flaw

   3 mos unrepaired weather buoy; $1.25M award (SEN 10 5) [NY Times 13 Aug 85]
** 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);
** 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.
** 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)
** 747SP (China Air.) autopilot tried to hold at 41,000 ft after engine failed,
   other engines died in stall, plane lost 32,000 feet [19 Feb 85] (SEN 10 2)
** 767 (UA 310 to Denver) four minutes without engines [August 1983] (SEN 8 5)
* F18 missile thrust while clamped, plane lost 20,000 feet (SEN 8 5)
* Mercury astronauts forced into manual reentry (SEN 8 3)
* Cosmic rays halve shuttle Challenger comm for 14 hours [8 Oct 84] (SEN 10 1)
* Frigate George Philip fired missile in opposite direction (SEN 8 5)
$ Hurricane Gloria in NY closes Midwest Stock Exchange (SEN 11 1)
$S Debit card copying easy despite encryption (DC Metro, SF BART, etc.)
$S Microwave phone calls easily interceptable; portable phones spoofable
$S Sputnik frequencies triggered garage-door openers

 ------------------------------ SOFTWARE -----------------------------------
!$ 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]
*$ Mariner 1: Atlas booster launch failure DO 100 I=1.10 (not 1,10) (SEN 8 5)
*$ Mariner 18: aborted due to missing NOT in program (SEN 5 2)
*$ F18: plane crashed due to missing exception condition, pilot OK (SEN 6 2)
*$ F14 off aircraft carrier into North Sea; due to software? (SEN 8 3)
*$ F14 lost to uncontrollable spin, traced to tactical software (SEN 9 5)
*$ El Dorado brake computer bug caused recall of all El Dorados (SEN 4 4)
$$ Viking had a misaligned antenna due to a faulty code patch (SEN 9 5)
$$ First Space Shuttle backup launch-computer synch problem (SEN 6 5 [Garman])
* Second Space Shuttle operational simulation: tight loop upon cancellation of
   an attempted abort; required manual override (SEN 7 1)
* Second Shuttle simulation: bug found in jettisoning an SRB (SEN 8 3)
*$ Delays of two Discovery shuttle launches due to backup computer outage
   [most recently 25 Aug 85] (SEN 10 5) [NY Times 26 August 1985]
* Shuttle STS-6 bugs in live Dual Mission software prevented aborts (SEN 11 1)
* Gemini V 100mi landing err, prog ignored orbital motion around sun (SEN 9 1)
* F16 simulation: plane flipped over whenever it crossed equator (SEN 5 2)
* F16 simulation: upside-down F16 deadlock over left vs. right roll (SEN 9 5)
* Nuclear reactor design: bug in Shock II model/program (SEN 4 2)
* Reactor overheating, low-oil indicator; two-fault coincidence (SEN 8 5)

```
*  SF BART train doors sometimes open on long legs between stations (SEN 8 5)
$  IRS reprogramming delays; interest paid on over 1,150,000 refunds (SEN 10 3)
$  $32 BILLION overdraft at Bank of New York (prog counter overflow) (SEN 11 1)
*S Numerous system intrusions and penetrations; implanted Trojan horses; 414s;
   intrusions to TRW Credit Information Service, British Telecom's Prestel,
   Santa Clara prison data system (inmate altered release date) (SEN 10 1).
   Computerized time-bomb inserted by programmer (for extortion?) (10 3)
   PC Graphics program Trojan horse (ArfArf) wiped out users' files (SEN 10 5)
*$ 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)
*  Multipatient monitoring system recalled; mixed up patients (SEN 11 1)
*  Pacemaker locked up when being adjusted by doctor (SEN 11 1)
*  Diagnostic lab instrument misprogrammed (SEN 11 1)
 S Chernenko at MOSKVAX: network mail hoax [1 April 1984] (SEN 9 4)
 S VMS tape backup SW trashed disc directories dumped in image mode (SEN 8 5)
*$ C&P computer crashes 44,000 DC phones (SEN 1 1)
$  1979 AT&T program bug downed phone service to Greece for months (SEN 10 3)
$  Demo NatComm thank-you mailing mistitled supporters [NY Times, 16 Dec 1984]
$  Slow responses in Bankwire interface SW resulted in double posting of tens
   of $millions, with interest losses (SEN 10 5)
$  Program bug permitted auto-teller overdrafts in Washington State (SEN 10 3)
 - Quebec election prediction gave loser big win [1981] (SEN 10 2, p. 25-26)
 - Other election problems including mid-stream corrections (HW/SW) (SEN 10 3)
 - SW vendor rigs elections? (David Burnham, NY Times front page, 29 July 1985)
 - Alaskan DMV program bug jails driver [Computerworld 15 Apr 85] (SEN 10 3)
 - Vancouver Stock Index lost 574 points over 22 months -- roundoff (SEN 9 1)
 - Gobbling of legitimate automatic teller cards (SEN 9 2, another SEN 10 5)

 ------------------------ HARDWARE/SOFTWARE -------------------------------
!  Michigan man killed by robotic die-casting machinery (SEN 10 2, 11 1)
!  Japanese mechanic killed by malfunctioning Kawasaki robot (SEN 10 1, 10 3)
   [Electronic Engineering Times, 21 December 1981]
!  Chinese computer builder electrocuted by his smart computer. (WWN headline:
  "Jealous Computer Zaps its Creator" after he built newer one!!)  (SEN 10 1)
*  FAA Air Traffic Control: many computer system outages (e.g., SEN 5 3)
*  ARPANET ground to a complete halt [27 Oct 1980] (SEN 6 1 [Rosen])
*$ Ford Mark VII wiring fires: flaw in computerized air suspension (SEN 10 3)
$S Harrah's $1.7 Million payoff scam -- Trojan horse chip (SEN 8 5)
$  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)
$  NY Stock Exch. halted for 41 minutes; drum channel errors killed primary
   and backup computer systems [24 Feb 72]
 - SF Muni Metro: Ghost Train reappeared, forcing manual operation (SEN 8 3)
*$ 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)
 S 1984 Rose Bowl hoax, scoreboard takeover ("Cal Tech vs. MIT") (SEN 9 2)

 ------- COMPUTER AS CATALYST, HUMAN FRAILTIES, OR UNKNOWN CAUSES -----------
!!$ Korean Airlines 007 shot down [1 Sept 1983], killing 269; autopilot left on
   HDG 246 rather than INERTIAL NAV? (NYReview 25 Apr 85, SEN 9 1, SEN 10 3)
!!$ Air New Zealand crashed into mountain [28 Nov 1979]; computer course data
   error had been detected and fixed, but pilots not informed (SEN 6 3 & 6 5)
!  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)
```

```
*  Unarmed Soviet missile crashed in Finland.  Wrong flight path? (SEN 10 2)
*$ South Pacific Airlines, 200 aboard, 500 mi off course near USSR [6 Oct 1984]
*S San Francisco Public Defender's database accessible to police (SEN 10 2)
*  Various cases of false arrest due to computer database use (SEN 10 3, 11 1)
*  Avionics failed, design used digitized copier-distorted curves (SEN 10 5)
$  .5M transaction became $500M, due to "000" convention; $200M lost (SEN 10 3)
$  Possible fraud on reinsurance -- message time stamp faked??? (SEN 10 5)
$  N-step reinsurance cycle; SW checked only N=1 and 2 (SEN 10 5)
*  FAA Air Traffic Control: many near-misses not reported (SEN 10 3)
!$$ Shuttle Challenger explosion, 7 killed.  Cause not yet known. [29 Jan 86]

 --------------- ILLUSTRATIVE OF POTENTIAL FUTURE PROBLEMS ------------------
*S Many known/past security flaws in computer operating systems and application
   programs.  Discovery of new flaws running way ahead of their elimination.
*  Expert systems in critical environments: unpredictability if (unknowingly)
   outside of range of competence, e.g., incompleteness of rule base. StarWars
$S 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]
   [These were only marginally computer-related, but suggestive.  Others
   are known, but not publically acknowledged.]

 --------------------- REFUTATION OF EARLIER REPORT -------------------------
* "Exocet missile not on expected-missile list, detected as friend" (SEN 8 3)
  [see Sheffield sinking, reported in New Scientist 97, p. 353, 2/10/83];
  Officially denied by British Minister of Defence Peter Blaker
  [New Scientist, vol 97, page 502, 24 Feb 83].  Rather, sinking abetted by
  defensive equipment being turned off to reduce communication interference?

[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 2: Issue 2

Saturday, 1 Feb 1986

Contents

More on Shuttle destruct systems

"MARTIN J. MOORE" <mooremj@eglin-vax>

This morning I talked to my successor at the Cape, who was in the Range Safety area during the launch. I've got a few things to report and some questions to answer from previous issues. I found out that the Range Safety Officer commanded the destruction of the SRBs approximately 20 sec after the main explosion, as they were careening wildly away from the site. Both SRBs did explode on command. The mood at the Cape is described as "devastated", especially among those who went outside to watch live. My successor also reported that Range Safety had been officially cleared as of yesterday, with respect to any responsibility for the accident; but that they expected *much* closer scrutiny than before (which is, of course, perfectly fine.) Interestingly, many of the media and a large percentage of the general public were not aware of the existence of the destruct system.

The latest theory I have heard contains a "leak" in one of the SRBs resulting in a 6000 C jet of flame cutting into the tank and igniting its fuel.

Now, individual responses:

> From: John Carpenter
> As I read the article [by Martin Moore in RISKS-1.43,] it occurred to me
> that as we discuss the risks of the destruct system we could be creating
> another risk by revealing the nature of it's operation...
> If the destruct system is public information, I would like to know why,
> If it isn't, it certainly has no place on the net.

Your point is well taken, and I did have some misgivings about posting the original article; not because I was revealing anything I shouldn't, but because I have no wish to be drawn into a national media controversy. Hence the restrictions on dissemination of the article. None of the information in the article was classified, and all of it was publicly available; and NASA is very good about providing access to any information that isn't classified. As to *why* it is public information...I think Neumann's response in 1-45 sums this up pretty well. Also, if it's not public, then the question that will be raised is "what are they hiding?"

Incidentally, my successor told me that there is an article in this morning's (1/31) Orlando Sentinel about the destruct system, at about the same level of detail as my article in 1-43. Would some Central Florida reader be kind enough to send me a summary or a copy of that article?

> From: Jeff Siegal <JBS%DEEP-THOUGHT@mit-eddie.MIT.EDU>
> Is there someone who knows enough about the security at NASA/KSC to be
> able to estimate the difficulty that a malicious party would have in
> getting getting physical access to the shuttle/SRB/MFT prior to the launch?

I'm not a physical security expert, but I believe that it would be extraordinarily difficult to get physical access to the shuttle itself at any time. Regarding the possibility raised by Kyle of a rifle shot, NASA maintains a "clear zone" 1.5 miles (I think) in radius around the shuttle when it is on the pad. This includes the closing of a public beach while the shuttle is on the pad, invariably causing complaints from some local citizens.

> From: b-davis@utah-cs.ARPA (Brad Davis)
> It also brings up an important question. If the hardware system is
> redundant, what about the software system? Is the same software running
> on all of the redundant hardware systems or are there more than one
> software packages developed. If there is only one software package then
> if one system fails due to a software failure then the other systems'
> software may fail since the same conditions may still be in effect.

Each member of a redundant set runs the same software (obviously, computers with different functions run different software). The danger you note is a real one; however, I believe the best solution is to make each piece of software as robust and fail-safe as possible. Consider that if redundant computers were running different software, you could have a failure of computer A and switchover to computer B without being able to reliably predict what computer B was doing at that instant! The whole idea of redundancy is that if a tool breaks in my hand, I want to be able to slap another one of the same kind of tool into my hand and not miss a beat. What your point leads to is to have additional tools for cases where the first one doesn't apply; this is a good idea, but it actually falls under the heading of "robustness" rather than "redundancy."

mjm

Re: Possible triggering of the self-destruct mechanism & (non)accident

Sean Malloy <malloy@nprdc.arpa>
Fri, 31 Jan 86 07:05:50 pst

>Date: 30 Jan 86 09:23:53 PST (Thu)
>From: Peter G. Neumann <Neumann@SRI-CSL.ARPA>
>Subject: Possible triggering of the self-destruct mechanism

[The physicist ... who speculated that the explosion in the solid-fuel rocket booster set off the self-destruct mechanism ... suggested that it could not have been a hydrogen leak because hydrogen burns clear and the Shuttle explosion had an obvious orange glow] is a classic example of what happens when people overspecialize themselves. Here we have a physicist making inaccurate statements about a fact of chemistry. I would suggest that this physicist watch the film of the Hindenberg disaster, and watch the bright, opaque flames of hydrogen burning in an insufficient quantity of oxygen for complete consumption. Only when hydrogen has a sufficient quantity of oxygen to burn completely does it burn with a clear blue flame.

One of the problems that this brings up is the tendency of the average person to regard any statement made by a scientist about a scientific subject as being correct because "they've been trained in science, so they know what they're talking about", whether they are making a statement within their field or out of it. Particularly when a scientist says that something is impossible or impractical. Too many scientists over history have delcared something impossible or impractical that is commonplace today to reject some line of research because of such pronouncements.

>Date: Thu 30 Jan 86 20:22:37-EST
>From: Jeff Siegal <JBS%DEEP-THOUGHT@mit-eddie.MIT.EDU>
>Subject: The Challenger [non]accident

>I have heard speculation that some fuel leaking (LHY or LOX) from the
>MFT and a unexpected flame could be seen (on slow-motion videotape)
>for some time prior to the explosion. This seems consistent with
>rifle bullet impact/puncture, long before the actual explosion
>occured.

This is one of the possibilities that the NASA investigating board is going to be looking at. However, the existence of the flames in the turbulent area just aft of the external tank is also consistent with a leak in the fuel pipes from the external tank to the orbiter.

If it did occur from an external impact, then the leak would have to have started after the shuttle had taken off, because the plume of escaping LHY would have caused enough condensation to be visible on the gantry monitors, a situation that would have halted the launch. I don't know of any way that someone shooting at the shuttle could be sure that the bullet would only damage the tank enough to fail at max Q, rather than penetrate and start a leak immediately. Or, failing that, to hit the external tank after launch, with the shuttle rolling and pitching into its climb attitude.

Sean Malloy
(malloy@nprdc-arpa)

Re: Possible triggering of the self-destruct mechanism

Brint Cooper <abc@BRL.ARPA>
Fri, 31 Jan 86 9:54:00 EST

But the news has consistently been reporting that, after the explosion that destroyed Challenger, the Air Force used the destruct mechanism to destroy the boosters (?) because one had gone off course and threatened populated areas. If this is true, can we not assume that the destruct mechanism did not cause the accident? Is it not a 'one time only' capability?

Brint

[As Martin Moore said in RISKS-1.43, there are FIVE destruct receivers: one on the ET and two on each of the SRBs. I was talking about the one on the ET; the SRBs somehow survived until they were intentionally destroyed. PGN]

The Challenger [non]accident

Herb Lin <LIN@MC.LCS.MIT.EDU>
Fri, 31 Jan 86 10:41:51 EST

> From: Jeff Siegal <JBS at DEEP-THOUGHT.MIT.EDU>
> I have heard speculation that some fuel leaking (LHY or LOX) ...
> ... This seems consistent with rifle bullet impact/puncture, long before the actual explosion occured.

Depends on what you mean by "long". The licks of flame at the base of the SRB occurred at most 2 sec before the main explosion. It was going at 2900 fps, so at best its altitude would have been 1 nautical mile lower when the bullet hit, meaning 8 nm altitude. Pretty far out to imagine a rifle bullet hitting at that point.

> There has been no public mention of the possibility of terrorism.

Terrorists claim credit for events. To my knowledge, no one has claimed credit.

Redundancy

<dcook@SCRC-STONY-BROOK.ARPA>
Fri, 31 Jan 86 10:49 EST

There is a point in the redundancy argument that has bothered me since I interviewed at Stratus a year or so ago.

Using the Stratus example, they run two copies of what they call a dipole. One copy is "live" and one is shadowing the live one. Each dipole is two mirror image processors with a high-speed comparator in the middle. When the live module gets a miscompare, it lights a LED and hands control over to the backup module. The operating system is able to do whatever clean up has to be done to brief module 2 so that computing is essentially non-stop. (Oh, one little "goodie" is that the module connectors are designed so that *the customer* can pull out the lighted module and put in a new one without shutting off the machine.) Now the $64,000 question: isn't the compare logic a single point of failure? (Note that because in this example you have a total of 4 CPU's, this isn't necessarily a crash.) But in the shuttle version, as I understood it, the systems were only redundant and therefore a comparator or checker failure could, it seems, knock the system out.

Galileo Plutonium power

Martin Schoffstall <schoff%rpics.csnet@CSNET-RELAY.ARPA>
Fri, 31 Jan 86 09:56:32 EST

I'm not sure how much information is publicly available on the generating systems of various satellites but I would like to point out something that has been published that is somewhat analogous: cardiac pacemakers.

As I remember it the plutonium powered ones were designed such that the containment device could not be penetrated by:

- .38 special at 15 feet.
- cremation temperatures (natural gas)
- aircraft impact.

Obviously I am being very coarse here and I don't have the details but I'm sure others do but if the above is "close" I'll throw out some number estimates that I'm sure others will correct:

- .38 special at 15 feet, say 1000 feet/sec 300 foot-lbs???
- natural gas burns at 2000 degrees?
- say 9gs at impact?

The point is as follows: If pacemakers are designed to handle stresses such as that I would assume that the satellites are designed much better, especially since the Soviets dumped a load on Canada (did they ever pay damages for that?).

marty schoffstall

Galileo Plutonium power

<James.Tomayko@a.sei.cmu.edu>
Friday, 31 January 1986 13:41:14 EST

Re Larry Shilkoff's note on Galileo carrying plutonium:

Not only plutonium, but the spacecraft was to be deployed atop a new version of the Centaur hydrogen/oxygen upperstage used on the Atlas-Centaur and Titan III boosters. Therefore, aside from several hundred pounds of plutonium the Shuttle would be carrying several thousand pounds of highly volatile fuel <inside> the cargo bay, adding considerable energy to any explosion. Worse yet, Galileo was to be the <first> user of the new upperstage, which shares little with its predecessor except the name. It has new tanks, engines, and instrumentation. In contrast to previous unmanned missions, only <one> Galileo has been built. Considering that the cost of building a second one would only have been 15% of the cost of the first, NASA is taking a big chance by launching its only Jupiter orbiter on an untested upperstage, in view of the multiple failures of Shuttle-carried upperstages such as the IUS and various satellite kickstages.

Sadly, the Galileo launch has already been delayed several years for various reasons (including one to switch it from the IUS to Centaur) and is likely to be delayed again. If the Shuttle fleet is not declared spaceworthy by May, the precession of Jupiter dictates a 13-month launch delay. Some of the parts of the spacecraft are nearly six years old now, and many have been in test for years on end. Even though the mission is projected to be shorter than Voyager, the spacecraft itself may actually "live" longer.

As a footnote specific to the risks question, a friend of mine who is a an astronaut trainer for NASA said to me several months ago that crews training for Galileo and the Solar Polar launch also using Centaur were wary because of critical questions relating to aborts. If the Shuttle has to do a return to launch site abort or an abort to Africa before deploying Galileo, what are the dangers of trying to land with a full load of hydrogen and radioactive isotopes? The possibility of explosions never came up. Now it has to.

VDT's and birth defects in mice

Dan Hoey <hoey@nrl-aic.ARPA>
31 Jan 1986 17:45:15 EST (Fri)

Yesterday I heard a radio report that a Swedish study found that video display terminals increased the incidence of birth defects in mice. Does anyone have more information on this?

I have not previously heard of any controlled research in the area that has identified a hazard. I am interested in trying to find out what the results of the study indicated, whether it is a new result, and how credible it is.

Dan

ORCON dissemination constraint on RISKS 1.43

<TMPLee@DOCKMASTER.ARPA>
Fri, 31 Jan 86 23:35 EST

You realize, of course, that Martin Moore's fascinating and worthwhile piece is accessible to *ANYONE* on the net who is allowed to use FTP by their home site since SRI-CSL supports anonymous FTP logons and since you have the RISKS back-issues in a public file.

> [... or indeed from any BBOARD receiving RISKS,
> not even necessarily on the ARPANET! PGN]

Ted

(For readers not familiar with it, ORCON is a handling marking in some circles that means "further distribution only with permission of the originator, i.e., ORiginator CONtrolled." It is a non-trivial task to get a computer system to implement that handling marking in a secure but natural way, especially across a network.)

> [Yes, of course. Less obscurely, someone can even ask to be put on the RISKS list, which I presume would permit me to send them the back issue within the spirit of Martin's constraints. I think what Martin may have been more concerned about was wholesale rebroadcastings. So what we have is an experimental exercise in self-control, to see if our network community is mature enough to adhere to his constraints. I would be very interested in hearing of any postings contary to his caveat. But you are very correct in suggesting that enforcing ORCON is a nasty problem that cannot be adequately addressed in most computer system environments today. That is one reason why overclassification occurs. 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 2: Issue 3

Saturday, 1 Feb 1986

Contents

Re: The possible vs the impossible

Dave Parnas <vax-populi!dparnas@nrl-css.arpa>
Sat, 1 Feb 86 08:52:11 pst

In response to an off the cuff remark by an unnamed physicist, Sean Malloy writes, "Too many scientists over history have declared something impossible or impractical that is commonplace today to reject some line of research because of such pronouncements." It is equally true that, too many scientists over history have declared to be possible or practical something that was later found to be impossible or impractical to pursue some line of research or development because of such pronouncements." There have been countless schemes to build perpetual motion machines, faster than light transport, 600 user time-sharing systems, world champion chess programs, unbreakable codes, impregnable forts, unsinkable ships, etc. etc.

We cannot reject a negative prediction simply because earlier negative predictions have been wrong just as we cannot reject a positive prediction simply because earlier positive predictions have been wrong. To have credence any prediction must be supported by detailed argumentation. If nobody can produce a convincing refutation of that argumentation, it is foolish not to act on the prediction. I would not support any effort to build faster than light rockets until someone shows me the flaw in Einstein's reasoning. Any researchers who hope to execute the following algorithm, "for I:=1 step 1 until 10,000 do `build rocket with n stages using DoD funding' should begin with a serious study of relativity, not with an SDI proposal to build a national totem pole center.

David L. Parnas

RISKS generalizations

Jim Horning <horning@decwrl.DEC.COM>
1 Feb 1986 1339-PST (Saturday)

Thanks for the digest of the digest. In following Risks from day to day, it was easy to lose sight of the general principles illustrated by all the specific cases and discussions. I guess that I would add to your list just one more generalization, concerning our ability to predict failures:

> If a system is complex, it is practically impossible to predict its sources of catastrophic failure. This is especially true in well-engineered systems, since good engineers make allowance for the problems that they foresee.

Jim H.
[Jim, That is perhaps the most important of all. Thanks. Peter]

Re: Challenger speculation

<ihnp4!utzoo!henry@ucbvax.berkeley.edu>
Sat, 1 Feb 86 05:11:33 PST

Herb Lin writes:

> If you are into pure, unadulterated speculation, another possibility
> is that a bullet was fired into an SRB while it was on the ground, and
> lodged there. When the fuel burned to that point, a jet leaked out,
> and triggered an explosion.

Alas for this particular speculation, the SRB fuel burns outward from the booster axis rather than upward along the booster. Combustion starts from a hole running the full length of the axis, and reaches the outer casing only at the very end of the burn. There may well be a few places near the ends where casing is progressively uncovered -- I don't have drawings at hand to check on this -- but this imposes much more severe constraints on aim. All in all, it seems implausible. All the more so because the SRBs continued on after the explosion, reasonably intact with no signs of any marked side thrust or substantial extraneous exhaust jets.

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

Re: Possible triggering of the self-destruct mechanism

Don Wegeng <Wegeng.Henr@Xerox.COM>
1 Feb 86 12:24:16 EST (Saturday)

I heard on CNN last night that one of the latest theories about the cause of the shuttle accident is that flames from a leak in an SRB may have set off the explosives which are part of the ET self-destruct mechanism. Not knowing anything about explosives, this seems plausible to me.

On the other hand, PBS interviewed someone last night (the editor of an aviation magazine, I believe) who said that a fuel leak in an SRB would have probably caused it to immediately stray wildly from its previous trajectory, but that the video of the launch seems to show both of them continuing on in the same general direction after the explosion. I believe that Range Safety did not destroy the SRBs until about 20 seconds after the explosion.

/Don

Redundancy in the Shuttle's Computers

Mark S. Day <MDAY@XX.LCS.MIT.EDU>
Sat 1 Feb 86 12:58:03-EST

A submission in RISKS-2.2 was concerned about a Stratus-like comparator mechanism being a single point of failure in the Space Shuttle's operations. However, the space shuttle's redundant set doesn't use a comparator mechanism. Instead, the actuators are controlled by a hydraulic "force-fight" mechanism, with each computer sending independent commands on independent buses. If one computer of four fails, the other three can exert enough force to overpower its (presumably bad) commands. If this pressure differential persists for long enough, the overpowered one is hydraulically bypassed.

For more details, see "Case Study: The Space Shuttle Primary Computer System" by Al Spector and Dave Gifford in CACM 27 #9 (September 1984).

--Mark

Galileo Plutonium power

Herb Lin <LIN@MC.LCS.MIT.EDU>

Sat, 1 Feb 86 11:15:38 EST

From: Martin Schoffstall

Icing the Shuttle

"Jim McGrath" <MCGRATH%OZ.AI.MIT.EDU@XX.LCS.MIT.EDU>
Sat 1 Feb 86 19:16:42-EST

> From: Werner Uhrig <CMP.WERNER@R20.UTEXAS.EDU>
> From TV-news coverage, I have the impression as if there might not
> have been adequate attention paid to icing which is supposed to
> have occurred this morning on the launch-pad.

My understanding was that the shuttle launch was delayed for more than an hour due to the icing. Since they delayed the launch specifically because of the weather, I strongly doubt that they would have delayed it for too short a period (if they are going to be yelled at by the media for being overly cautious, then they might as well delay for the full required time).

Jim

[This subject drifts somewhat from the computer-related risks. However, because we have to train ourselves to think about vulnerabilities overall, I have included Jim's message. Jim, note the various reports of icicles. 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 2: Issue 4

Sunday, 2 Jan 1986

Contents

Solid propellants

Mike McLaughlin <mikemcl@nrl-csr>
Sun, 2 Feb 86 14:08:17 est

Odd topic for a computer centered forum - but worth discussing a bit. The computer hook relates to what could have been monitored, detected, and reacted to in computer time; but not in human time. I base this discussion on long-ago experience in writing about solid propellant rockets, plus Sunday's TV & radio news.

1. Solid propellants burn at a surface. If they are designed to burn at one end, they are called "cigarette burning." If they are designed to burn through a hole in the middle, they are not. The prepared hunk of propellant is called a "grain."

2. Cigarette burning produces roughly constant propelling force throughout the burn. Chunks of loose propellant (cylinders, spheres, etc.) produce more thrust at the beginning, less at the end, as the surface area of the grains is reduced/consumed.

3. The hole in the center of a grain can be tailored in shape to affect burn characteristics just about any way the engineer wants. In addition, "inhibitors" can be put on the grain to further control its burn characteristics.

4. In most boosters the grain fills the container, except for the hole in the center, and a space near the nozzle. An ignitor (actually, another small rocket) is usually at the end opposite the nozzle.

5. Remember, the grain burns at the surface. A crack in the grain provides another surface to burn. If the grain separates from the casing, the exterior of the grain provides another burning surface. If the grain is sectional, i.e. too large to build as one unit, the ends of the sections can provide burning surfaces. Naturally, it is the engineer's job to control and prevent these undesirable burning surfaces, and to produce the thrust profile required for the task at hand.

(tutorial ends, speculation begins)

It is my understanding that "SRBs" were built in 6 sections, and assembled on-site. Nose, 4 grain sections (not necessarily identical, the hole can be tapered), and tail. I also understand that the casing sections were "bolted" together (probably a fairly complex bolting system); and were considered to be quite safe & reliable. The casings were recovered after a launch, refurbished, reloaded, & re-used.

Recently released film, computer-enhanced offline, after the accident, show that the right hand SRB had a plume coming out the side, in a location that appeared to me to be about where the joint between the 3rd and 4th grain/ casing sections would be - but, depending on the actual design, could have been further aft, near the end of the grain, towards the nozzle. If this was a casing/grain burn-through, the mildest result would be assymetric thrust. *This should have been immediately detectable by the guidance system's reaction in attempting to maintain the desired trajectory.* If similar perterbations occurred in wind shears, etc., it might not be recognizable as abnormal.

Another result could be that the errant jet impinged on the main fuel tank, heating, penetrating, and igniting the fuel load. (It might be able to ignite it without penetrating the tank structure.) *This should be quickly detectable by excursions in tank pressure.* Reaction times, even of computers, might not be fast enough to make any difference in the outcome.

I believe that both of the above could have been detected with instrumentation that was certainly on board. Additional (or existing?) instrumentation could detect temperature changes in SRB and fuel tank skins, torques on SRB mounts, abnormal "seismic" vibrations within the SRB structure, abnormal "plumes", etc.

It is so easy to second-guess. I am sure the engineers concerned are castigating themselves for what they failed to forsee, for what they concluded was trivial, for what now seems eminently clear to them. I wish they would quit it. The whole program is so full of checks and balances that only a Higher Power could add more. From "MTM's" description of the safety system, it seems a miracle that it was possible to destroy the SRBs under normal circumstances, much less in the middle of disaster. The astronauts participated in the design and manufacturing process - they were ready to go.

We have lost seven of our best and brightest. But perhaps we are seven closer to whatever is out there in space, waiting for us to get on with it, get out there, fulfill our dreams.

Peter: this is too long, but I had to write it, tell someone. I went into space in the '50s, with Heinlein and Bonestell. The Challenger Seven must not be regarded as sacrifices on the altar of science - they were just seven of us who went a little closer to the edge of knowledge than the rest of us dare. The human/computer symbiosis will get us out there eventually, and the Challenger Seven will have helped every one who follows them. - Mike

Plutonium

"Jim McGrath" <MCGRATH%OZ.AI.MIT.EDU@XX.LCS.MIT.EDU>
Sat 1 Feb 86 19:20:51-EST

First, I assume that everyone knows that no atomic explosion would occur under any circumstances. Nor any fallout.

That only leaves the actual radioactive fuel itself. Plutonium's danger, for a constant mass, depends upon the size of the particles. The worse thing that can happen is for dust size particles to be inhaled. Large chunks would be a local danger, but one easily handled. Note that if the launch was from the Cape, then it would eventually settle into the ocean. This would aid considerably in dispersing it to extremely low concentrations. Finally, remember that the Soviets lost a satellite powered by radioactives over Canada. While the Canadians were not happy, and took clean up measures, the real problem was getting the Soviets to pony up for the cleanup costs.

> From: James.Tomayko@a.sei.cmu.edu
> .... Therefore, aside from several hundred pounds of plutonium ...

Are you sure about your numbers? Hundreds of pounds of pure plutonium? The cost would be outrageous. Moreover, this implies a total mass would be thousands of pounds, if not tons (since the plutonium would be diluted to a lower concentration and sufficient shielding for the electronics would have to be provided). Maybe you mean a fuel assembly massing hundreds of pounds? If so, then the actual mass of Plutonium would be a small fraction of the total mass.

Jim

SRB Self-Destruct Mechanisms

Clive Dawson <AI.CLIVE@MCC.ARPA>
Fri 31 Jan 86 13:29:44-CST

One aspect of the SRB self-destruct mechanism which has bothered me the most is the fact that a single action will destroy BOTH SRB's (and perhaps the external tank as well?). It is clear that recovery of the intact casings would have been invaluable in the NASA investigation. News reports tell us that one of the SRB's was headed on a dangerous course toward popluated areas and had to be destroyed. Fair enough. But why destroy the other one unless and until it was also proved necessary??

Thinking about this further reveals it may not be that simple. First of all, I can imagine scenarios in which both SRB's would need to be destroyed as quickly as possible, especially in the early phases of the launch. You would certainly want to have a mechanism for doing this as exists now. On the other hand, last Tuesday's events show that it would be very valuable to be able to destroy them individually as well. This would imply modifying the hardware/software such that each SRB responded to two sets of tones: a common set for both and an individual set. Perhaps a simpler scheme would be to simply have two different frequencies which could be used simultaneously or separately.

Those of us discussing this were momentarily satsified until somebody asked, "Yes, but how do you tell which SRB is which??!" In this case, it was reasonably easy to answer that question when they emerged from the fireball, but this might not always be the case. Furthermore, it's not clear that the task would be any easier when watching them on a radar screen. (What does the Range Safety Officer use?) This difficulty can presumably be overcome by electronic equipment on each SRB that would tag its radar image in some fashion.

I'm wondering if this is a case of "good hindsight", or if there are other considerations we didn't think of.

Clive

Details on the 1981 Quebec election -- a program bug (RISKS-2.1)

Jean-Francois Lamy <lamy%utai%toronto.csnet@CSNET-RELAY.ARPA>
02 Feb 86 09:40:43 EST (Sun)

> [FROM THE SUMMARY OF DISASTERS in RISKS-2.1:]
>
> - Quebec election prediction gave loser big win [1981] (SEN 10 2, p. 25-26)

Election monitoring software for two television networks was faulty: votes were being attributed to the wrong candidates. Names were being kept in alphabetical order while votes were kept in decreasing order.
This is a language related bug: the contractor was IP Sharp and the software was programmed in APL -- the informations ended up in distinct vectors, with one being mistakenly kept sorted.

Jean-Francois Lamy
Department of Computer Science, University of Toronto,
Departement d'informatique et de recherche operationnelle, U. de Montreal.

CSNet: lamy@toronto.csnet
UUCP: {utzoo,ihnp4,decwrl,uw-beaver}!utcsri!utai!lamy

CDN: lamy@iro.udem.cdn (lamy%iro.udem.cdn@ubc.csnet)

[FOR THE RECORD, HERE WAS THE ORIGINAL PARAGRAPH from Software Engineering Notes, from a review by PGN of John Shore's "The Sachertorte Algorithm and Other Antidotes to Computer Anxiety", vol 10 no 2, pp. 25-26, April 1985.]

The chapter on Myths of Correctness brings us the tale of the 1981 provincial election in Quebec, Canada. One station's computer had been misprogrammed, and it announced that the overwhelming underdog Union Nationale had won 19 out of 49 races. Their announcers somehow even managed to come up with erudite analyses explaining why this amazing upset had occurred. It was not until twenty minutes after the other station had declared that the Parti Quebecois and the Liberal Party had totally dominated the election that the first station realized that there had been a colossal mistake somewhere!   [PGN]

Search RISKS using swish-e

Search RISKS using swish-e

THE RISKS DIGEST

Forum on Risks to the Public in Computers and Related Systems

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

Volume 2: Issue 5

Monday, 3 Jan 1986

Contents

Sean Malloy <malloy@nprdc.arpa>
Mon, 3 Feb 86 07:14:54 pst

Subject: Solid Propellants and What the Computers Should Monitor

>Date: Sun, 2 Feb 86 14:08:17 est
>From: mikemcl@nrl-csr (Mike McLaughlin)
>Subject: SRBs and What the Computers Should Monitor

>Another result could be that the errant jet impinged on the main fuel tank,
>heating, penetrating, and igniting the fuel load. (It might be able to ignite
>it without penetrating the tank structure.) *This should be quickly detec-
>table by excursions in tank pressure.* Reaction times, even of computers,
>might not be fast enough to make any difference in the outcome.

>I believe that both of the above could have been detected with instrumentation
>that was certainly on board. Additional (or existing?) instrumentation could

>detect temperature changes in SRB and fuel tank skins, torques on SRB mounts,
>abnormal "seismic" vibrations within the SRB structure, abnormal "plumes",
>etc.

One of the points that was brought up during the broadcasts the day of the disaster was that the telemetry tapes were going to have to be analyzed to determine if there was any indication as to what happened. The temperature data for the external tank was specifically mentioned as one of the telemetry streams that was NOT fed to a display in either the launch control area or Mission Control. The NASA spokesman explained that there was so much information coming in that a decision had to be made to limit what the launch control personnel had to pay attention to.

This brings up a much more subtle problem in risk evaluation -- what data is considered relevant to the task at hand? A line has to be drawn between significant and extraneous data, based on the processing capacity of the system/personnel interpreting the data. NASA had decided that the ET temperatures were not of immediate use to the launch control personnel, and simply recorded the data. In the previous 24 shuttle launches, they were right; in this case, they were wrong. In the future, they probably will have someone monitoring that data. What also has to be considered in the decision is what can be done on the basis of a given stream of data. I don't know how long the ET temperatures would have been elevated before the explosion, so I don't know whether there would have been time to recognize the problem, identify the source, and jettison the SRBs. If you can show that there won't be enough time to react properly, then giving someone responsibility for making the right decision in that situation is asking someone to volunteer to have a nervous breakdown.

In retrospect, there should have been immediate scrutiny of the SRB performance. Looking at the pictures of the exhaust trails after the explosion, one of the SRBs is looping away from the blast apparently undamaged, while the trail from the other proceeds straight for a short distance, then peters out abruptly. Why would one survive unscathed while the other one was badly damaged unless something happened with or adjacent to the SRB? Hindsight is always 20/20.

Sean Malloy
(malloy@nprdc-arpa)

Charley Wingate <mangoe@mimsy.umd.edu>
Mon, 3 Feb 86 14:00:39 EST

Subject: SRBs and What the Computers Should Monitor
Organization: University of Maryland, Dept. of Computer Sci.

> If this [new plume]
>was a casing/grain burn-through, the mildest result would be assymetric
>thrust. *This should have been immediately detectable by the guidance
>system's reaction in attempting to maintain the desired trajectory.* If
>similar pert[u]rbations occurred in wind shears, etc., it might not be

>recognizable as abnormal.

In fact, the shuttle was just passing out of an area where wind shear is common. If you look at the trail that was left, there appears to be a sharp jog just before the plume enters the base of the fireball cloud, suggesting either wind shear or perhaps the thrust from the extra hole. It's also possible that the thrust from the spurious plume would be too small to be noticed (which I believe is in this case a matter of several percent).

>Another result could be that the errant jet impinged on the main fuel tank,
  [... see above message ...]

Judging from the film, this seems unlikely, although localized overheating could have occured and caused a failure.

>Those of us discussing this were momentarily satsified until somebody
>asked, "Yes, but how do you tell which SRB is which??!" ...

Actually, the shuttle is within visual range throughout the SRB boost phase, if I remember correctly. The two boosters could be distinguished by painting a different roll pattern on each.

As far as risks are concerned, I think that the one point of all of this is to illustrate the value of collecting data even if you can't immediately use it to determine what to do. There seems to be a consensus, for instance, that temperature readings on the ET and the removed sensors on the SRBs were useless under normal circumstances. It was immediately apparent how valuable they would be in illuminating the failure that did finally occur. It will be interesting to see if NASA's philosophy changes as a result of the accident.

Charles Wingate

Bill Keefe <keefe%milrat.DEC@decwrl.DEC.COM>
Monday, 3 Feb 1986 07:45:51-PST

Subject: SRB survival

That both SRB's survived, while the shuttle didn't, makes me wonder how the structural integrity of the SRB's differed from the shuttle in allowing them to survive the explosion.

- Bill Keefe

Tim Wicinski <wicinski@nrl-css.ARPA>
Mon, 3 Feb 86 07:41:52 est

Subject: Physical Security at the Cape

I believe someone asked about the security out at the Cape, I have some good
first hand knowledge about it. I have been to over a half dozen launches
and/or attempted launches at the Cape, and I worked there for a few months
as a Contractor during a few launches. A few days before a launch the Air
Force closes off the beaches north of the Cape for a good distance (over 3
miles) as well as some of the beaches south of the Cape. I believe they try
to keep visitors away from the launch site at a distance of about 4 miles,
which is is how far away you see the launch if you get a car pass from Nasa.
The press and VIP's sit only 2.3 miles from the launch pad, and they have a
hard time from the guards getting there (I once viewed the launch from
here). Also, planes are allowed in a restricted air space around the Cape,
but you are still a good distance from the launch itself, and with Air Force
jets patrolling the area to make sure of this.

On launch days when I worked at the Cape, I usually had my car searched,
and a few times they put in spot check points to make sure no one was going
where they weren't supposed to. At every launch the security I felt was
very good, but I guess there is always somewhere where there could be
a place where someone could get in undetected, it is a big place.

--tim wicinski@nrl-css {umcp-cs decvax}!nrl-css!wicinski

A hard rain is gonna fall.

Marc Vilain <MVILAIN@G.BBN.COM>
Mon 3 Feb 86 15:18:48-EST

To: risks@SRI-CSL.ARPA

Larry Shilkoff observed in RISKS 1-45 that future shuttle missions have
(or maybe had) been planned to carry plutonium-powered spacecraft, the
Galileo probe in particular. Had Challenger carried such a spacecraft,
Southern Florida would have been exposed to substantial plutonium fallout.

This brings up a similar issue with the Strategic Defense Initiative. In
a recent Forum article in New Scientist (16 January 1986), physicist Raymond
Harrowell considered the after-effects of a *successful* interception of
Soviet ICBM boosters. He looked at the levels of radioactive fallout that
would ensue from the return to Earth of disabled ICBMs and their warheads.
Quoting from his article:

> Some simple calculations indicate the likely consequences of SDI
> interceptions of Soviet ICBMs. A Soviet first strike could involve the
> simultaneous launching of some 5000 nuclear warheads at targets in the US.
> If only 20 percent of these warheads, each containing 10 kg of plutonium
> 239, are disintegrated (without a nuclear explosion) in the northern
> hemisphere, about 10^13 lethal doses (if inhaled or ingested) of
> alpha-emitting plutonium would be released -- about 5,000 doses per person
> in the northern hemisphere. If that radioactive debris were distributed
> uniformly, there would be one lethal dose for every 25 square metres of the
> northern hemisphere. Not all the radioactive material will have immediate

effects on Earth but, however delayed the fallout of stratospheric plutonium might be, its long half-life (24,000 years) would ensure its eventual arrival at altitudes likely to be occupied by human beings, other animals and plants.

Most of the technical discussion of the risks in deploying the SDI has focussed on its failure modes. Harrowell's analysis brings up another face of the problem, namely that the success mode of the system may be so narrowly defined as to ensure significant, if not unacceptable, risks -- whether the system succeeds or fails.

The regrettable lesson, is that success of an engineering application, if defined overly narrowly, may not be success at all.

marc vilain.

PS: Full reference to the article: Raymond Harrowell, "Debris that shatters the star wars myth", _New Scientist_, 16 January 1986, page 55.

<James.Tomayko@a.sei.cmu.edu>
Monday, 3 February 1986 11:40:09 EST

Subject: Correction re Galileo plutonium

Re my post dated 31 January:

>...aside from several hundred pounds of plutonium.....(onboard Galileo)

Make that 24 pounds---sorry for the mistatement.

Quebec Election

Dan Craigen <CMP.CRAIGEN@R20.UTEXAS.EDU>
Mon 3 Feb 86 14:43:55-CST

To: risks@SRI-CSL.ARPA

Naturally I was somewhat interested in Lamy's comments on the Quebec election (1981) and I.P. Sharp's role. I was only marginally aware of the details involved and thought I should check the facts.

[Dan is at IPSharp. PGN]

Lamy is essentially accurate in his comments. His message does, however, seem to indicate that there was an error in the APL language interpreter. Such was not the case -- it was a programming error.
A case could possibly be made that the programming styles that have developed around the APL notation led to the resulting situation. (But there are always penalties that arise from using any notation...)

dan

SCRIBE time-bomb goes off!

Peter G. Neumann <Neumann@SRI-CSL.ARPA>
Mon 3 Feb 86 02:05:07-PST

To: RISKS@SRI-CSL

At the same time over the past weekend, SCRIBE stopped working on several (but not all) SRI computer systems. There was some sort of accidental latent time-bomb in the UNILOGIC software (other than the expected annual crypto-lock time-bomb that goes off annually to prevent people from merrily copying SCRIBE and using it indefinitely or without paying their dues).
This is a fine example of software that has always worked suddenly no longer working.

Peter

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

Index to Volume 1

Saturday, 31 May 1986

  - Some financial disaster cases from Software Engineering Notes (three contributions, totalling five reports)

- Volume 1 Issue 12 (13 Sep 85)
  - Wire-Transfer Risks; Risk of Non-application of Technology (Jerry Saltzer)
  - Date-Time stamps (and errors therein) (Ted M P Lee)
  - JMC's remarks (Joseph Weizenbaum)
  - Subjective Factors in Risk Assessment (Lynne C. Moore)
  - Moral vs. Technological Progress (Charlie Crummer)
- Volume 1 Issue 13 (15 Sep 85)
  - Risks in RISKS (Peter G. Neumann)
  - Preserving rights to Email messages (Larry Hunter)
  - Risk Comparisons (T. Tussing)
  - Risks history/philosophy (Nicholas Spies) [long but interesting]
- Volume 1 Issue 14 (16 Sep 85)
  - Pitfalls of a Fail-Safe Mail Protocol? (Peter G. Neumann)
  - Some Ruminations on an Ideal Defense System (Bob Estell)
  - SDI, feasibility is irrelevant (Gopal)
- Volume 1 Issue 15 (20 Sep 85)
  - SDI Panel at 8th ICSE in London (David Weiss)
  - Risks to the Moderator (PGN)
  - Mailer Protocol Woes (Marty Moore)
  - Another Horror Story -- Sidereal Time Rollover (Marty Moore)
  - Article: Health Hazards of Computers (Ted Shapin)
  - Two More SDI Related Queries (douglas schuler)
  - CAL ID -- computerized fingerprint system (douglas schuler)
- Volume 1 Issue 16 (26 Sep 85)
  - Intellectual honesty and the SDI (Bill Anderson)
  - RISKy Stuff (Mike Padlipsky)
  - Mailer Protocol Woes (Rob Austein)
  - Risks in Synchronizing Network Clocks (Ann Westine for Jon Postel)
  - Re: Moral vs. Technological Progress (Joel Upchurch)
  - Risk Contingency Planning -- Computers in Mexico (Mike McLaughlin)
- Volume 1 Issue 17 (27 Sep 85)
  - SDI debate announcement
  - Minor risk to the pocket book (Eugene Miya)
  - Social Impacts of Computing: Graduate Study at UC-Irvine (Rob Kling)
  - Friendly enemy test teams (John Mashey)
  - More protocol goofs (Dave Curry)
- Volume 1 Issue 18 (4 Oct 85)
  - Lack of a backup computer closes stock exchange (Marty Moore)
  - DPMA survey on computer crime offenses (J.A.N. Lee)
  - Ethics vs. morality (Marty Cohen)
  - The Mythical Man-Month of Risk (Stavros Macrakis)
  - Risk Assessment by real people (Mike McLaughlin)

CRTs again, solution to one eye-problem (Mike McLaughlin)
- Failure of Mexican Networks (Dave Flory)
- Technical Reports Lists (Laurence Leff)

- Volume 1 Issue 19 (8 Oct 85)
    - Emanations and interference in the civil sector (Peter Neumann,Jerry Saltzer)
    - Administrivia -- Escaped Mail and Delays (Mark S. Day)
    - Computer databases (Andy Mondore)
    - Re: Friendly test teams (John Mashey)
    - Re: CRTs again, solution to one eye-problem (Brint Cooper)
- Volume 1 Issue 20 (8 Oct 85)
    - Risks using robots in industry (Bill Keefe)
    - Re: Computer databases (Matt Bishop)
    - Registrar's databases; Database risks - census data (Hal Murray, 2 messages)
    - The winners of evolution... (William McKeeman)
- Volume 1 Issue 21 (10 Oct 85)
    - Public Accountability (Jim Horning, Peter Neumann)
    - The Titanic Effect (JAN Lee)
    - Databases, Grades, etc. (Brian Borchers, Andy Mondore, Mark Day [twice], Alan Wexelblat, Ross McKenrick, Randy Parker)
- Volume 1 Issue 22 (9 Nov 85)
    - Administratrivia (Friedrich von Henke)
    - Medical software incidents (Nancy Leveson)
    - European activities (Udo Voges)
    - Robots are different (Jerry Saltzer)
    - Automobile computer control systems (Bennett Smith)
    - Police computers (Dave Dyer)
    - Electronic Surveillance (Geoffrey S. Goodfellow / Bill Keefe)
    - Network Mailer Woes (Lynne Moore)
    - Databases, grades, etc. (Karl Kluge, Andy Mondore, Mark Sienkiew)
- Volume 1 Issue 23 (19 Nov 85)
    - Expecting the unexpected (Peter G. Neumann)
    - Safety Group Activities in the U.S. (Nancy Leveson)
    - Automobile computer control systems susceptible to interference(Bennett Smith)
    - Irresponsible computer "game"; BBS Legislation (Ted Shapin)
    - SDI Debate at MIT (John L. Mills)
- Volume 1 Issue 24 (20 Nov 85)
    - Doing Something About Risks in Computer Systems (Brad Davis)
    - Space Program Software (Jerome Rosenberg)
    - Susceptibility to interference (John Brewer)
    - Expecting the unexpected (Herb Lin)
    - Philip W. Anderson's "Case Against Star Wars" (Pete Kaiser)
- Volume 1 Issue 25 (1 Dec 85)
    - Some Thoughts on Unpredicted Long-Term Risks (Peter G. Neumann)

Computer snafu halts treasury (Peter G. Trei)
- "Hacker" Game (Ken Brown; Keith F. Lynch; Werner Uhrig)

Volume 1 Issue 26 (4 Dec 85)

- Humility (Matt Bishop)
- Reliable Computer Systems (Jim Horning)
- Electromagnetic Interference (Peter G. Neumann)
- Hackers (Thomas Cox)
- "The Hacker Game": Is it simulating security of *REAL* machines? (Ted Shapin)
- Unexpected load on telephone trunks (Ted Shapin)

Volume 1 Issue 27 (7 Dec 85)

- Contents: SPECIAL ISSUE on viruses and worms

Volume 1 Issue 28 (9 Dec 85)

- Viruses and Worms (Mark S. Day, Aaron M. Ellison, Ted Lee, Dave Parnas)
- Electromagnetic Interference (Chuq Von Rospach)
- Crackers (Peter Reiher, Matt Bishop, Dave Dyer)

Volume 1 Issue 29 (12 Dec 85)

- Computer-compared prescriptions (Dave Platt)
- SDI: Danny Cohen and Eastport Group comments (Gary Chapman via Jim Horning)
- Worms, etc. (Keith F. Lynch, Stavros Macrakis)
- Passwords, etc. (King Ables, Dave Curry, Dan Bower)

Volume 1 Issue 30 (16 Dec 85)

- Request for Cases, Settled or Decided (George S. Cole)
- Risks of job displacement from computerization (Fred Hapgood)
- Risks re computer-compared prescriptions (Richard Lamson)
- Legal bootlegs (a case against worms) (K. Richard Magill)
- Passwords ()
- Verifying source code vs. executable code (Martin J. Moore)
- Seminar - SDI Debate (SU) (Joan Feigenbaum)

Volume 1 Issue 31 (19 Dec 85)

- Enough on passwords? Pharmacy systems (Elizabeth Willey)
- Risks re computer-compared prescriptions (Brint Cooper)
- Oops (Marty Moore)
- $32 Billion Overdraft Resulted From Snafu (Washington Post)

Volume 1 Issue 32 (23 Dec 85)

- Can Bank of New York Bank on Star Wars? (Jim Horning)
- Cohen's AT&T SDI Software Analogy (Richard A. Cowan)
- Failure probabilities in decision chains (Will Martin)
- Ten-year any-worseries (Dan Hoey)
- Multiple digests as a result of crashed systems (Rob Austein)

Volume 1 Issue 33 (1 Jan 86)

- Star Wars and Bank of NY (Brint Cooper, Chris Hibbert, Jim Horning)
- Lipton and SDI (Herb Lin)

  - The robot sentry (Martin Minow)
  - Murphy is watching YOU (Rob Austein)
  - Re: Failure probabilities in decision chains (Stephen Wolff)

- Volume 1 Issue 34 (4 Jan 86)

  - C&P Computer Problems Foul 44,000 D.C. Phones (Mike McLaughlin)
  - Putting the Man in the Loop; Testing SDI; Independent Battlestations (Jim McGrath)
  - Failure probablities in decision chains... independence (Edward Vielmetti)
  - Pharmacy prescription systems (Normand Lepine)
  - Masquerading (Paul W. Nelson)

- Volume 1 Issue 35 (6 Jan 86)

  - SDI -- Meteors as substitutes for nuclear war (Jim Horning, Dave Parnas) Putting a Man in the Loop (Jim McGrath, Herb Lin, JM again) Testing SDI (Herb Lin, Jim McGrath, HL again) Independent Battlestations (Herb Lin, Jim McGrath, HL again) The Goal of SDI; Politicians (Jim McGrath)
  - Pharmacy prescription systems (Rodney Hoffman)
  - How to steal people's passwords (Roy Smith)

- Volume 1 Issue 36 (7 Jan 86)

  - PLEASE READ Weapons and Hope by Freeman Dyson. (Peter Denning)
  - Wolves in the woods (Jim Horning, Dave Parnas)
  - "Certifiable reliability" and the purpose of SDI (Michael L. Scott)
  - SDI Testing (Jim McGrath, Jim Horning)
  - Dec. 85 IEEE TSE: Special Issue on Software Reliability--Part I
  - Masquerading (R. Michael Tague)

- Volume 1 Issue 37 (9 Jan 86)

  - IEEE TSE Special Issue on Reliability -- Part 1 (Nancy Leveson)
  - SDI Testing (Nancy Leveson, Dave Parnas)
  - Multiple redundancy (Henry Spencer)
  - On Freeman Dyson (Gary Chapman, Jon Jacky)

- Volume 1 Issue 38 (9 Jan 86)

  - Ad-hominem SDI discussion (Mike McLaughlin [and Peter Neumann])
  - Men in the loop (Martin J. Moore)
  - Failure probabilities in decision chains (Jim Miller) [also in SOFT-ENG]
  - Testing SDI (Karl Kluge, Robert Goldman)
  - Summing Up on SDI (Jim McGrath)

- Volume 1 Issue 39 (13 Jan 86)

  - Real-time responsibility (Dave Wade)
  - Big Brother (Jim McGrath, Peter Neumann)
  - Men in the SDI loop (Herb Lin)

- Volume 1 Issue 40 (17 Jan 86)

  - Big Brother (Jim Ziobro, Keith Lynch)
  - Multiple redundancy (Henry Spencer)
  - COMPASS 86: System Integrity: Process Security and Safety (Al Friend)

- Volume 1 Issue 41 (19 Jan 86)

- On a Clear Day You Can See Forever ... or Nothing At All (Peter G. Neumann)
- Unreleased SDIO Computing Panel Report: Specialists Fault `Star Wars' Work
- Man in the loop and magnetic bottles (Jon Jacky)

● Volume 1 Issue 42 (28 Jan 86)

- The Space Shuttle Challenger (Peter G. Neumann)
- When you start an engine at 40 below, you could be injured... (David Wade)
- "Brazil" and Risks to the Public (Martin Minow)

● Volume 1 Issue 43 (29 Jan 86)

- Reliability of Shuttle Destruct System (Martin J. Moore) (LONG MESSAGE)
- Challenger lost (and note on self-destruct mechanism) (Earle S. Kyle, jr.)
- Challenger ICING !!! (Werner Uhrig)
- Big Brother, again (Col. G. L. Sicherman)

● Volume 1 Issue 44 (29 Jan 86)

- Shuttle SRB/MFT self-destruct mechanisms (Dusty Bleher, Herb Lin, Martin Moore)
- Challenger speculation (Herb Lin)

● Volume 1 Issue 45 (31 Jan 86)

- Risks from discussing Reliability of Shuttle Destruct System (John Carpenter, Peter G. Neumann)
- Possible triggering of the self-destruct mechanism (Peter G. Neumann)
- Challenger and Living with High-Risk Technologies (Dave Benson)
- The Challenger [non]accident (Jeff Siegal)
- Shuttle Explosion -- Plutonium on Galileo (Larry Shilkoff)
- Reliability in redundant systems (Brad Davis)

Search RISKS using swish-e

Report problems with the web pages to the maintainer

THE RISKS DIGEST

Forum On Risks To The Public In Computers And Related Systems

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

Search RISKS using swish-e [ ]

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

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

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

Feeds

RSS 1.0 (full text)

RSS 2.0 (full text)

ATOM (full text)

RDF feed

WAP (latest issue)

Simplified (latest issue)

Smartphone (latest issue)
Under Development!!

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

Please 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 3

Sunday, 2 November 1986

  - An additional SDI problem: sensor technology (Eugene Miya)
  - Privacy in the electronic age (Dave Platt)
  - Sgt York software (Larry Campbell, Mark Vilain)

- Volume 3 Issue 7 (13 Jun 86)
  - Eastport Study Group report ("Science" article) (Pete Kaiser)
  - An additional SDI problem: sensor technology (Jon Jacky)
  - Shuttle software and CACM (James Tomayko [and Herb Lin])
  - Privacy laws (Bruce O'Neel)
  - A mini-editorial on running the RISKS Forum (PGN)

- Volume 3 Issue 8 (15 Jun 86)
  - Challenger, SDI, and management risks (Dick Dunn)
  - Re: Risks from inappropriate scale of energy technologies (Chuck Ferguson)
  - Distributed versus centralized computer systems (Peter G. Neumann)
  - Privacy legislation (Michael Wagner)

- Volume 3 Issue 9 (20 Jun 86)
  - Informing the Senate on SDI (Jim Horning)
  - A medical risk of computers (Karen R. Sollins)
  - Risks of VDTs (Alan Wexelblat)
  - Minor addition on Risks of Distributed Energy (Ted Lee)

- Volume 3 Issue 10 (20 Jun 86)
  - Re: Privacy Legislation & Cellular Swiss Cheese (RISKS-3.8)(Geoff Goodfellow)
  - Re: Privacy Legislation (RISKS-3.6) [divulging] (Dan Franklin)
  - Re: Privacy Legislation (RISKS-3.6) [radar detectors] (Herb Lin)

- Volume 3 Issue 11 (23 Jun 86 [mislabelled RISKS-3.12 in masthead])
  - A medical risk of computers (overdose during radiation therapy) (Jon Jacky)
  - Secure computer systems (Herb Lin)
  - Radar Detectors (Re: Privacy legislation in RISKS-3.10) (Jeff Makey)
  - Telco Central office woes in Southfield, MI. (via Geoff Goodfellow)
  - Reducing the managerial risks in SDI (Bob Estell)
  - Economic Impact of SDI: Transcript Info (Richard A. Cowan)

- Volume 3 Issue 12 (24 Jun 86)
  - License Plate Risks (Chuck Price)
  - SDI is for ICBMs, Not Terrorists (Mark Day)
  - Still another kind of clock problem (Rodney Hoffman)
  - Estimating Unreported Incidents (Ken Laws)
  - Estimating Unreported Incidents -- and the risks of using statistics (PGN)
  - Re: Privacy legislation (RISKS-3.8) and radio eavesdropping (Jerry Mungle, Jeff Mogul, Jim Aspnes)

- Volume 3 Issue 13 (26 Jun 86)
  - The Risky Gap Between Two Design Cultures (Jack Goldberg)
  - Risks of nuclear power (Dan Franklin)
  - Research programs that pay for themselves (Rich Cowan)
  - Having an influence from "within the system" (Rich Cowan)
  - RISKS in running RISKS -- continued (PGN and an unhappy Mailer)

- Volume 3 Issue 14 (27 Jun 86)
    - A Personal View on SDI (Harlan Mills)
    - Privacy legislation (RISKS-3.10) (Jerome H. Saltzer)
    - Risks in burning wood (Mike McLaughlin)
    - Mailer explosion (Sean Malloy)
- Volume 3 Issue 15 (29 Jun 86)
    - A Personal View on SDI from Harlan Mills (Herb Lin)
    - Having an influence from "within the system" (Herb Lin)
    - Re: Research programs that pay for themselves (Rich Cowan)
    - Text Scanners (Fred Hapgood)
- Volume 3 Issue 16 (30 Jun 86)
    - Chernobyl (a suprise to the Soviets) (Martin Minow)
    - Airwaves & Security (2 Subjects) (Richard S. D'Ippolito via dhm)
    - Interesting Technical Questions (originally SDI) (Martin Moore)
- Volume 3 Issue 17 (3 Jul 86)
    - How Much Computer Literacy Is Enough? (JAN Lee)
    - Working within the system (Rich Cowan)
    - Re: [Airwaves &] Security -- SDI (Herb Lin)
    - Complex issues, complex answers (Bob Estell)
    - Politics and Engineering Practice (Seifert)
    - Multiple copies of RISKS-3.16 (Kenneth Sloan)
    - GTE Sprint billing problems (Chuck Weinstock/Lee Breisacher)
- Volume 3 Issue 18 (8 Jul 86)
    - Computer Crime in Scandinavia (Martin Minow)
    - Re: Risks from inappropriate scale of energy technologies (Henry Spencer)
    - Sensor technology and disinformation (Eugene Miya)
    - Educating to prevent RISKS (Steven Gutfreund)
    - Rash of 'Undeliverable mail' (Chuck Price)
- Volume 3 Issue 19 (10 Jul 86)
    - Computer Literacy (Rick Smith, Bob Estell, Col. G. L. Sicherman, PGN)
- Volume 3 Issue 20 (15 Jul 86)
    - Risks of computer incompetence (Dave Benson)
    - RE: educating about RISKS (Don Lindsay)
    - Computer Literacy (RISKS-3.19) (Ron Morgan) ... and Basic (Martin Minow, Andrew Klossner, PGN)
    - Dial-up computing (Sterling Bjorndahl)
    - Research programs that pay for themselves (Clayton Cramer)
- Volume 3 Issue 21 (16 Jul 86)
    - Responsibility (Willis Ware)
    - Programming languages and computer literacy (Bob Estell)
    - Teaching about risks, BASIC, NASA, etc. (Eugene Miya)
    - Programming Languages (Matthew Kruk)
    - BBoard Lingo (Trojan viruses,...) (Hank Burchard, via Peter G. Neumann)

- Volume 3 Issue 22 (19 Jul 86)
    - Nostalgia (Mike Williams)
    - Flames about BASIC (Jim Anderson)
    - More on risks of teaching "just" programming (Herb Lin)
    - Responsibility for Computer Actions (George S. Cole)
    - CDP and Certification (Andy Glew)
    - The undetected hang-up risk (more) (Ted Lee)
- Volume 3 Issue 23 (22 Jul 86)
    - Re: Comet and Electra (Jim Horning)
    - 100,000 Late Phone Bills (Mike McLaughlin)
    - Types of "Programming" (Henry Schaffer)
- Volume 3 Issue 24 (24 Jul 86)
    - Comet and Electra (Jerry Saltzer, Marv Zelkowitz, Don Chiasson, Bard Bloom)
    - No gasoline because the computer is down? (Jim Barnes)
    - HBO Hacker Captain Midnight Caught (via Geoff Goodfellow)
- Volume 3 Issue 25 (24 Jul 86)
    - Petroski on the Comet failures (Alan Wexelblat)
    - Re: Comet and Electra (Douglas Adams)
    - On the dangers of human error (Brian Randell via Lindsay Marshall)
    - Software Paranoia (Ken Laws)
    - Royal Wedding Risks (Lindsay Marshall)
    - How to Think Creatively (John Mackin)
    - Dangers of improperly protected equipment (Kevin Belles)
- Volume 3 Issue 26 (26 Jul 86)
    - DIVAD (Herb Lin)
    - Royal wedding risks -- common change modes (Don Chiasson)
    - Security and dialbacks (David I. Emery via Herb Lin) [Long message]
- Volume 3 Issue 27 (29 Jul 86)
    - Whoops! Lost an Area Code! (Clayton Cramer)
    - Comet-Electra (RISKS-3.25) (Stephen Little)
    - Comparing computer security with human security (Bob Estell)
- Volume 3 Issue 28 (31 Jul 86)
    - Laserprinter dangers (Mansfiel)
    - Errors in error-handlers (Mansfiel)
    - Military testing errors (Alan Wexelblat)
    - Re: Comet-Electra (RISKS-3.25) (Bill Fisher)
    - Computer and Human Security (Lindsay Marshall)
- Volume 3 Issue 29 (1 Aug 86)
    - Ozone hole undetected for years due to programming error (Bill McGarry)
    - Aircraft simulators and risks (Art Evans)
    - Military testing errors (Scott E. Preece)
    - Risks: computers in the electoral process (Kurt Hyde via Pete Kaiser)
    - Risks of CAD (Alan Wexelblat)

- Volume 3 Issue 30 (4 Aug 86)
  - Ozone hole undetected (Jeffrey Mogul)
  - Re: Risks of CAD (Henry Spencer)
  - Comment on Hartford Civic Roof Design (Richard S D'Ippolito)
  - Expert system to catch spies (Larry Van Sickle)
- Volume 3 Issue 31 (5 Aug 86)
  - Another cruise missile lands outside Eglin test range (Martin J. Moore)
  - Aircraft simulators and risks (Gary Wemmerus)
  - Re: Comment on Hartford Civic Roof Design (Brad Davis)
  - Expert system to catch spies (RISKS-3.30) (Chris McDonald)
  - Computer and Human Security (Henry Spencer)
  - Ozone Reference (Eugene Miya)
  - Financial risks (Robert Stroud)
  - Mail Load Light(e)ning? (SRI-CSL Mail Daemon)
- Volume 3 Issue 32 (6 Aug 86)
  - DC-10 Crash (Chuck Weinstock)
  - Earthquake Reporting (AP)
  - The Recent Near-Disaster for the Shuttle Columbia (Peter G. Neumann)
  - Traffic lights in Austin (Alan Wexelblat)
  - Re: Laserprinter dangers (Graeme Hirst)
- Volume 3 Issue 33 (7 Aug 86)
  - Air traffic computer failure (Hal Perkins)
  - Re: Laserprinter dangers (Sean Malloy)
  - Re: Expert system to catch spies (Rich Kulawiec)
  - Survey of Computer Professionals (Kurt Hyde)
- Volume 3 Issue 34 (9 Aug 86)
  - Non-Flying Airplanes and Flying Glass (Jim Horning)
  - Failure Recovery, Simulations, and Reality (Danny Cohen)
  - Ottawa Power Failure (Dan Craigen)
  - Liability for Software Problems (Peter G. Neumann)
  - Ozone hole (Hal Perkins)
  - Re: Survey of Trust in Election Computers (Chris Hibbert)
  - Nondelivery of RISKS-2.38 (8 April 1986) and other mail (Communications Satellite [and PGN])
- Volume 3 Issue 35 (11 Aug 86)
  - Flying windows on the Hancock Building (Remy Malan)
  - Pilots and counter-intuitive maneuvers (Martin Minow)
  - Mail adrift (Mike McLaughlin)
  - Laserprinter dangers (Niall Mansfield)
  - A bit of humor and even philosophy (Willis Ware)
  - Official Report on Chernobyl disaster (Robert Stroud)
- Volume 3 Issue 36 (12 Aug 86)
  - Another Medical Risk? (Lee Breisacher)
  - RISKy Business in Surgery (Mark Jackson)

  - Enlightened Traffic Management (Alan Wexelblat)
  - Flight Simulator Simulators Have Faults (Dave Benson)
  - Re: Flight Simulators and Software Bugs (Bjorn Freeman-Benson)
  - Always Mount a Scratch Monkey (Art Evans)
  - Re: supermarket crashes (Jeffrey Mogul)
  - Machine errors - another point of view (Bob Estell)
  - Human Behv. & FSM's (Robert DiCamillo)

- Volume 3 Issue 51 (7 Sep 86)

  - Computer almost created swing vote (Bjorn Freeman-Benson)
  - Computer Sabotage of Encyclopedia Brittania (Rosanna Lee)
  - F-16 software (Wayne Throop)
  - Arbiter failures and design failures (Martin Harriman)
  - Systems errors (hardware AND humans) (Bill Janssen)
  - Re: Terminal (!) lockup (Roy Smith)

- Volume 3 Issue 52 (8 Sep 86)

  - Re: F-16 software (Nancy Leveson)
  - Upside-down F-16's and "Human error" (Jon Jacky)
  - F-16 software (Scott E. Preece)
  - Do More Faults Mean More Faults? (Ken Dymond)
  - Why components DON'T interact more often (Bob Estell)
  - Computer almost created swing vote (Scott E. Preece)
  - Computer Sabotage [MISSING LAST LINE FROM RISKS-3.51]
  - Computer Sabotage of Encyclopedia Brittanica (Scott E. Preece)
  - Captain Midnight & military satellites (Werner Uhrig)
  - Re: always mount a scratch monkey (Alexander Dupuy)
  - Erroneous computer printout used in public debates (Chris Koenigsberg)

- Volume 3 Issue 53 (10 Sep 86)

  - Hardware/software interface and risks (Mike Brown)
  - More on Upside down F-16s (Mike Brown)
  - "Unreasonable behavior" and software (Gary Chapman)
  - Re: supermarket crashes (Scott Preece)

- Volume 3 Issue 54 (15 Sep 86)

  - Ada Inherently Secure? (Mike McLaughlin)
  - A million lines of code works the first time? (Ken Calvert)
  - Computers and Ethics (Mark S. Day)
  - New book: HUMAN RELIABILITY: With Human Factors (Elizabeth ?)
  - Answers to WWMCCS Intercomputer Network questions (Harold E. Russell)

- Volume 3 Issue 55 (15 Sep 86)

  - Hardware/software interface and risks (Kevin Kenny)
  - F-16 (Holleran, Eugene Miya, Ihor Kinal, Doug Wade)

- Volume 3 Issue 56 (16 Sep 86)

  - Massive UNIX breakins at Stanford (Brian Reid)

- Volume 3 Issue 57 (16 Sep 86)

  - Sane sanity checks / risking public discussion (Jim Purtilo)
  - More (Maybe Too Much) On More Faults (Ken Dymond)
  - Re: Protection of personal information (Correction from David Chase)
  - Towards an effective definition of "autonomous" weapons (Herb Lin, Clifford Johnson [twice each])

- Volume 3 Issue 65 (24 Sep 86)

  - UNIX and network security again (Andy Freeman)
  - F-16 software (Wayne Throop)
  - NYT feature article on SDI software (Hal Perkins)
  - Autonomous widgets (Mike McLaughlin)
  - Robottle Management Software? (PGN)

- Volume 3 Issue 66 (25 Sep 86)

  - Follow-up on Stanford breakins: PLEASE LISTEN THIS TIME! (Brian Reid)
  - F-16 software [concluded?] (Herb Lin)

- Volume 3 Issue 67 (25 Sep 86)

  - Old GAO Report on Medical Device Software (Chuck Youman)
  - Re: Stanford breakin, RISKS-3.62 DIGEST (Darrel VanBuer)
  - Re: Passwords and the Stanford break-in (RISKS-3.61) (Dave Sherman)
  - Re: role of simulation - combat simulation for sale (Jon Jacky)
  - MIT Symposium on economic impact of military spending (Richard Cowan)
  - "Friendly" missiles and computer error -- more on the Exocet (Rob MacLachlan)

- Volume 3 Issue 68 (26 Sep 86)

  - VDU risks -- Government changes its mind, perhaps (Stephen Page)
  - "Drive by wire" systems (Charles R. Fry)
  - Viking Landers worked the first time and met the specs (Dave Benson)
  - Unix breakins - secure networks (David C. Stewart)
  - Comment on the reaction to Brian's Breakin Tale (Dave Taylor)
  - Reliability, complexity, and confidence in SDI software (Bob Estell)

- Volume 3 Issue 69 (28 Sep 86)

  - Confidence in software via fault expectations (Dave Benson)
  - More on Stanford's UNIX breakins (John Shore, Scott Preece)
  - F-16 simulator (Stev Knowles)
  - Deliberate overrides? (Herb Lin)
  - Viking Landers -- correction to RISKS-3.68 (Courtenay Footman)

- Volume 3 Issue 70 (29 Sep 86)

  - Deliberate overrides? (Scott E. Preece)
  - Multiple causes and where to place the "blame" (PGN)
  - The Art of "Science" and its Computers (PGN)
  - No-lock Brakes (Peter Ladkin)
  - Sanity in Automating Keyword Abstracting (Brint Cooper)
  - The Network Is Getting Old? (PGN)

- Volume 3 Issue 71 (30 Sep 86)

  - Deliberate overrides? (Herb Lin, Alan M. Marcum, Eugene Miya)
  - "Friendly" missiles and computer error - more on the Exocet (Robert Stroud)

  - Re: Reliability, complexity, and confidence in SDI (Michal Young)
  - My understanding of "path" and "bathtub curve" (Bob Estell)
  - More artificial than intelligent? (Autokeywords) (Bob Estell)
  - A Viking lander query (PGN)
  - Note on ARPANET congestion (Nancy Cassidy)
  - Indeed, the network is getting old (Jonathan Young)

- Volume 3 Issue 72 (1 Oct 86)

  - Viking Lander (Nancy Leveson)
  - Deliberate override (George Adams)
  - Overriding overrides (Peter Ladkin)
  - A propos landing gear (Peter Ladkin)
  - Paths in Testing (Mark S. Day)
  - Confidence in software via fault expectations (Darrel VanBuer)

- Volume 3 Issue 73 (2 Oct 86)

  - Lessons from Viking Lander software (Bob Estell)
  - Software wears out? (Rob Austein)
  - Wrongful eviction through computer error (Bill Janssen)
  - Deliberate override (Herb Lin, Ray Chen)
  - Re: Piper Arrow Gear Override (Douglas Adams)
  - Undesirable breakins and causes (Ian Davis)

- Volume 3 Issue 74 (3 Oct 86)

  - Opinions vs. Facts in RISKS Reports (re Aviation Accidents) (Danny Cohen)
  - Mathematical checking of programs (quoting Tony Hoare) (Niall Mansfield)
  - Risks of maintaining computer timestamps revisited [RISKS-3.57] (Ian Davis)
  - Keyword indexing in automated catalogs (Betsy Hanes Perry)
  - Re: Viking Landers -- correction (Scott Preece)
  - Re: Confidence in software via fault expectations (Scott Preece)
  - Overrides and tradeoffs (Jerry Leichter)
  - Re: Deliberate overrides (Brint Cooper)
  - Re: idiot-proof cars (risks-3.68) (Col. G. L. Sicherman)

- Volume 3 Issue 75 (4 Oct 86)

  - re: Estell on Viking (RISKS-3.73) (David Parnas, Dave Benson)
  - Software becomes obsolete, but does not wear out (Dave Benson)
  - The fallacy of independence (Dave Benson)
  - Re: Paths in Testing (RISKS-3:72) (Chuck Youman, Mark Day)
  - Mathematical checking of programs (quoting Tony Hoare) (Henry Spencer)

- Volume 3 Issue 76 (5 Oct 86)

  - Obsolescence vs wearing out (RISKS-3.75) (Jerome H. Saltzer)
  - Cars, computers and unexpected interactions (Mike McLaughlin)
  - Re: Mathematical checking of programs (quoting Tony Hoare) (Matthew Wiener)
  - "Total correctness", "complete reliability" (RISKS-3.75) (Bard Bloom)

- Volume 3 Issue 77 (8 Oct 86)

  - Evaluating software risks (Brian Randell)
  - Misapplication of hardware reliability models (Nancy Leveson)
  - Deliberate overrides? (Mark Brader, Ephraim)

- (Voting) Machine Politics (Mike McLaughlin)
- Computer RISKS in "Ticker-Tape Parades" (PGN)
- SDI vs. Social Security (Scott Guthery)
- SDI Impossibility? (Scott Dorsey)
- Feeping Creaturism (Charley Wingate)

● Volume 3 Issue 91 (30 Oct 86)

- Evolution, Progress (Jim Horning)
- System Overload (David Parnas)
- "Perfect" systems from imperfect parts (Bob Estell)
- The software that worked too well (Dave Benson)
- Assessing system effectiveness (Dave Benson)
- Risks of raining computer print-out (Alan Wexelblat, Martin Ewing, PGN)

Search RISKS using swish-e

Report problems with the web pages to the maintainer

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 2: Issue 6

Tuesday, 4 Feb 1986

Contents

Shuttle computers

Marc Vilain <MVILAIN@G.BBN.COM>
Tue 4 Feb 86 12:34:09-EST

The following is excerpted from this Sunday's New York Times. It may be somewhat old news to some, but does a good job of summarizing much of the evidence and arguments surrounding the Challenger's computers.

SHUTTLE EXPERTS DOUBT COMPUTERS COULD DETECT FIRE
By David E. Sanger

The computers and sensors that guided the flight of the space shuttle Challenger appear not to have been programmed to detect flames burning throught the sides of a solid-fuel booster rocket, experts familiar with the shuttle system said yesterday.

Their comments came as evidence accumulated that the right-side booster began to fail as much as 10 seconds before the explosion that destroyed the craft, as reported yesterday in the New York Times.

Even if the sensors had picked up the first signs of fire, safety measures built into the system to protect the astronauts would have prevented the shedding of the giant external fuel tank that exploded soon after, NASA officials and the computers' designers said.

Only From Pilot

That command could have come only from the pilot, and officials said they doubted even that could have saved the crew.

...

Experts who have studied the shuttle's computer system say it was not programmed to separate the orbiter automatically from its fuel supply in part because of the fears that faulty sensor readings could cause the computers to abort a mission unnecessarily, risking the lives of the crew.

Preparation for Emergencies

Still the possibility that there were signs of trouble as long as 10 seconds before the explosion raised some questions yesterday about the enormously complex equipment that guides the shuttle.

...

"The possibility that a booster might burn through could well have been a failure mode that was never considered," said Alfred Spector, a Carnegie-Mellon professor who two years ago conducted a study of the computer system guiding the shuttle.

NASA officials said little publicly in response to the report that data sent from the shuttle showed a sudden drop in the power of the right booster rocket about 10 seconds before the spacecraft exploded.

But computer experts said the computer's response to such a power drop may have been executed flawlessly. The program, they said, was primarily designed to correct for the effects of an uneven rocket thrust by swiveling engine nozzles to the side, keeping the shuttle on course. Sources close to the situation say that the ground data show that the nozzles had in fact swiveled to one side.

In the absence of other danger signals, however, the computer would not have searched for the cause of the power loss. And the initial signals apparently indicated only a 4 percent decrease in thrust, a figure that the computer, or the cabin crew and officials at the Johnson Space Center in Houston, may have judged did not indicate a serious problem.

...

[End of excerpt]

SRBs and Challenger

Mike Iglesias <iglesias@UCI.EDU>
Mon, 03 Feb 86 21:06:59 -0800

According to this morning's LA Times:

- Early shuttle flights had sensors on the SRBs to monitor performance, but they were removed to save weight when it was felt that the SRBs were performing well. The sensors monitored pressure, temperature and vibration in the SRBs.

- Two Rockwell officials familiar with the NASA inquiry said that NASA data shows that the 3 main engines experienced a power loss just before the explosion. The power loss was noted between one-tenth and one-one hundreth of a second before the explosion. The SRB that probably caused the explosion suffered a 3% loss of power (about 100,000 pounds of thrust) seconds before.

- NASA noted that even if there were sensors on the SRBs, little can be done to save the crew if there is a problem during the first 2 minutes during the flight. They might be able to jettison the SRBs, but it would be difficult to stay clear of them and the external tank. And another NASA spokesman said later that the crews don't train for that maneuver, and that NASA documents state that such an escape is possible only after the SRBs have completed firing. The shuttle would have a near-impossible task of ditching in the ocean if it was able to steer clear of the SRBs and the ET.

- Other Rockwell sources said that telemetry shows that the external tank experienced an increase in pressure in both the oxygen and hydrogen tanks, and that pressure relief valves in both tanks popped to decrease some of the pressure.

Could the crew have survived had they known about the problem? Who knows? Maybe, if they had known about the SRB problem in time, if they had been able to get away from the SRBs and the ET, and been able to ditch successfully in the ocean. That's a lot of ifs...

I wonder if NASA is going to think twice about removing sensors after this...

Mike Iglesias
University of California, Irvine

Galileo, Plutonium, Centaur, physical security [4 messages combined]

<ihnp4!utzoo!henry@seismo.CSS.GOV>
Tue, 4 Feb 86 22:26:32 EST

[Re Marty Schoffstall, on plutonium batteries for pacemakers and satellites:]

Note that the Soviet satellites use reactors, not isotope capsules, as their power sources. The two are quite different, especially in this context. It's not practical to encapsulate a reactor the way the isotope capsules are armored against possible accidents.

[Re Larry Shilkoff, on Galileo:]

The capsules used to hold plutonium 238 (note that this is not the fissionable isotope used in reactors and bombs) for deep-space power sources are designed to withstand uncontrolled re-entry, and I think to withstand launch accidents as well. Quite likely they would have survived intact. There have been a few re-entries of satellites carrying such capsules, and one went into the Pacific with the lunar module of Apollo 13. No dire results.

[Re James Tomayko, on Centaur aboard shuttle:]

Apart from the volatility, this is nothing new: major solid-fuel motors routinely ride in the cargo bay. Those things are dangerous too. People doing some of the amateur-satellite work have estimated that the paperwork needed to clear a satellite for a ride in the shuttle cargo bay roughly triples if it is carrying any substantial rocket motor, solid or liquid.

> Worse yet, Galileo was to be the
> <first> user of the new upperstage, which shares little with its predecessor
> except the name. It has new tanks, engines, and instrumentation...

Not quite true: the Ulysses solar-polar mission, using the same upper stage, was to launch about a week before Galileo. Still awfully tight.

> [in an abort] what are the dangers of trying to land with a full load of
> hydrogen and radioactive isotopes? ...

Actually, although the liquid hydrogen is what everyone points at, the liquid oxygen is probably the greater danger. "Stages to Saturn", the NASA history of the Saturn boosters, commented that liquid hydrogen hazards were found to be comparable to those of highly-volatile gasoline (not trivial, mind you!), while it was liquid oxygen that really needed extraordinary handling precautions.

[Re: Jeff Siegal on NASA/KSC physical security:]

It's not conspicuous, but it's there. Practically nothing is said about it in public. I was down at the Cape for the 41C launch, on the National Space Institute tour. We got (I think) a slightly closer look at things than the ordinary KSC tours, but when we went past the actual active pad a day or two before launch we were cautioned that (a) the bus could slow down but it must not stop, and (b) all windows, including the driver's little vent window, must stay 100% shut. With a strong indication that we were being watched and our NASA guide would be in deep guano if either rule was violated even momentarily. We went past some press folks setting up cameras, and our guide commented "if you're wondering why they're allowed out of their bus and you aren't, it's because they've been searched and you haven't". The pad area proper also has an impressive concentration of things like concertina wire (think of it as industrial-strength barbed wire) around its perimeter. It's difficult for a non-professional to evaluate the quality of the precautions, but they did seem to be taking it seriously.

I have since heard a rumor that there were some awkward and hushed-up incidents quite early in the Shuttle program that caused considerable tightening of the original fairly loose security.

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

[We may be approaching the point of no return on some of the second- and third-order discussion. PGN]

Re: RISKS-2.5 & "Some simple calculations"

<Ayers.PA@Xerox.COM>
4 Feb 86 09:05:41 PST (Tuesday)

If we're going to talk about SDI and WWIII rather than computers,
please, let us at least use responsible analysis. Vilain quotes

> Some simple calculations indicate the likely consequences of SDI interceptions of Soviet ICBMs. A Soviet first strike could involve the simultaneous launching of some 5000 nuclear warheads at targets in the US. If only 20 percent of these warheads, each containing 10 kg of plutonium 239, are disintegrated (without a nuclear explosion) in the northern hemisphere, about 10^13 lethal doses (if inhaled or ingested) of alpha-emitting plutonium would be released -- about 5,000 doses per person in the northern hemisphere. If that radioactive debris were distributed uniformly, there would be one lethal dose for every 25 square metres of the northern hemisphere. Not all the radioactive material will have immediate effects on Earth but, however delayed the fallout of stratospheric plutonium might be, its long half-life (24,000 years) would ensure its eventual arrival at altitudes likely to be occupied by human beings, other animals and plants.

This arithmetic [of?] "simple calculations" is irrelevant. The "if"s are
totally bogus.

Every year, the US spreads about one fatal-dose per person of Arsenic
Trioxide onto food-plants via crop-dusters. And how many fatal doses of
salt does Connecticut spread on the roads every winter?

If you believe the quote, everyone in the northern hemisphere is already
dead (more than one fatal dose per person) from the atmospheric bomb
tests of the '50s and 60's.

Bob

A hard rain is gonna fall.

Herb Lin <LIN@MC.LCS.MIT.EDU>
Tue, 4 Feb 86 23:37:23 EST

risks@SRI-CSL.ARPA

From: Marc Vilain <MVILAIN at G.BBN.COM>

> This brings up a similar issue with the Strategic Defense Initiative.

> If that radioactive debris were distributed uniformly, there would be
> one lethal dose for every 25 square metres of the northern hemisphere.

Bad assumption. Most of boost-phase intercept occurs over the Soviet Union.

> The regrettable lesson, is that success of an engineering
> application, if defined overly narrowly, may not be success at all.

This general point is well-taken, despite my comments above. As they say, "The operation was a success but the patient died."

By the slip of a finger ... [A lesser risk]

<TMPLee@DOCKMASTER.ARPA>
Tue, 4 Feb 86 23:33 EST

I thought the following incident fits into RISKS. Recently one of our people moved from our Philadelphia corporate headquarters site (thousands of employees) to our new Atlanta Development Center (only dozen or so on board at the time.) He sent the appropriate change of address notifications into the publishers of his professional journals. ("change my address, P.O. Box xyz, Blue Bell, Pa., to P.O. Box qrs, Norcross, Ga.", or words close to that.) Shortly thereafter our poor office secretary and part-time mail clerk down there was inundated with mountains of journals from one of those publishers. We don't know exactly what happened, but apparently the software used to maintain the circulation list was instructed, and dutifully did so, to "change all addresses that match" (which, I guess, would be used to move a household) rather than "change this particular subscriber record": every single journal by that publisher addressed to our corporate headquarters (modulo spelling variations, I presume) had by a handful of keystrokes been redirected elsewhere. The publisher involved shall remain nameless (not ACM, that would make too nice a story) but it was one dealing with the computer field. The problem appears to have been fixed, naturally the fix taking the usual "six weeks", whereas the original error, naturally, happened in a couple of days.

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 2: Issue 7

Thursday, 6 Feb 1986

Contents

The lesson of Challenger

Barry Shein <bzs%bostonu.csnet@CSNET-RELAY.ARPA>
Tue, 4 Feb 86 22:39:47 EST

Although this is a very sad event, it would be sadder if we would refuse to learn from it.

Seven people were killed in this disaster, and billions of dollars of equipment, but the rest of us will survive. The lesson is the limit of faith we should put into our technology. I believe we should continue, that in many ways we have been too cautious and should heed the pioneering spirit we all feel, even if the pioneers put themselves at risk. Individuals should be allowed to risk something to gain something, they should be encouraged, applauded and honored for their sacrifices, if need be.

It is quite another thing to think that such systems can be relied upon to end the current nuclear nightmare, that in these technologies we will find strengths that we cannot find in ourselves at a bargaining table. In this case, we risk far too much.

The technology will fail, we should expect that and have the courage to take chances where there is something to learn. Only a fool or a madman would risk an entire civilization's fate on a gadget.

Let's continue into space, with all due speed. But let's also stop thinking that nations (people!) will settle their differences with gadgets. The philosopher's stone for human relations just doesn't exist.

-Barry Shein, Boston University

Mistaken Arrest due to computer error

Steve Rabin <stever%vlsi.caltech.edu@nrl-css>
Sun, 26 Jan 86 02:25:03 PST

Thursday night I was mistakenly arrested by a Pasadena police patrol due to a computer error. I spent two hours in a smelly holding cell while my friends collected bail. $130.50 Cash. Exact change please.

When I appeared in court Friday morning with proof that the ticket had in fact been paid in February of 1984, the case against me was dismissed.

In conversation with the court clerk and with the police officers who processed me I learned that mistakes like this are not uncommon, and that the safest thing for me to due is to keep the 1984 receipt on my person at all times. One friendly officer said "In processing these (warrant dismissals), the paperwork goes through so many hands that if anyone drops the ball there is no way to tell what happened."

It appears I have a good case against the City & County of LA ("failure to properly document computer system"), and the City of Pasadena ("improper stop and use of excessive force by arresting officer"). The excessive force claim arises because the officer physically prevented my departure after I had identified myself and before the information about the bogus warrant came over the radio. He is not supposed to do this. There may be an additional case against Pasadena if in fact the statute on the original offense (jay walking in 1981) had expired.

Do any of you high powered legal types have any insights on my case? Do any of you folks know good, reasonably priced lawyers in the LA area with whom you have had personal experience? Have their been any problems with Chas. & Angelique Johnson, attys? I am also looking for a good patent lawyer, so if you know/are one please write me.

My interest in this news group (until now) has been focused on copyright &

software marketing issues. I am a grad student in Computer Science at Caltech. Hobbies include science fiction, the tunes of Garcia/Hunter, and long distance running. I would like to do triathalons too but my swimming is weak. Pleased to meet you all.

("I won't do it again! Honest!")
(I thank you for your patience) stever@{cit-vax.arpa,csvax.caltech.edu}

[For those of you who have not read RISKS back to 4 September 1985, RISKS-1.5 contains several related items, another in RISKS-1.20. PGN]

Denial of [Religious] Service

Chris Guthrie <chris%ic%BERKELEY.EDU@nrl-css>
Tue, 31 Dec 85 20:55:34 PST

[This is an old item, but had not previously been reported here. The denial-of-service problem is very widespread, and presents much greater risks than most of us realize. PGN]

Reprinted from the Sacramento Bee:

ANGRY CALLER TITHES UP FALWELL'S LINE

A self-employed computer whiz in Atlanta is under orders from a telephone company to stop making harassing computerized calls to the Rev. Jerry Falwell's toll-free tithing line.

Officials of Southern Bell said they would yank Edward Johnson's service if he didn't unhook his phone from a computer that automatically dials Falwell's "Old Time Gospel Hour" every 30 seconds, tying up the line and annoying the operators.

Falwell aides said they would take legal action against him.

Johnson's computer has been making the calls to the Lynchburg, Va., line day and night since April. Officials estimated that the computer has made 500,000 calls to Falwell's line.

Johnson, 46, a computer analyst who said he wants to bog down Falwell's fund-raising operations and hurt the organization's morale, maintained that he is not impressed by the threats. He said he is considering moving his computer to a friend's telephone to continue the campaign.

Falwell aides said they would take legal action against Johnson, who started his crusade against Falwell after his mother "almost gave the family farm away" to the television evangelist.

Mark DeMoss, a Falwell assistant, said Falwell has lost a dollar for every call Johnson's computer has made.

"We do plan legal action," DeMoss said. "Naturally toll-free calls in that quantity would constitute a pretty significant expense for us."

Johnson's crusade stopped Friday at 11 a.m. when a Southern Bell security agent, acting on a complaint from Falwell's organization, called Johnson and ordered him to unhook his computer from his phone or lose his telephone service.

Earthquake Monitoring Systems

Gary T. Leavens <GTL@XX.LCS.MIT.EDU>
Thu 6 Feb 86 12:38:18-EST

I recently read an article in CACM about two earthquake monitoring networks in California. Presumably they are designed to withstand a major earthquake so they can perform their data collection functions, etc. Does anyone know if they really are designed to function during a major earthquake? If so, what design considerations were used?

Re: Mice & CRT Radiation

Ted Shapin <BEC.SHAPIN@USC-ECL.ARPA>
Wed 5 Feb 86 12:10:43-PST

John Ott, the pioneer in time lapse photography, published a paperback book "Health and Light" about 10 years ago. In it he mentioned his observations on the negative effects on the health of mice exposed to a color CRT, even when the screen was covered with black cardboard.
I don't recall any more than that.

Ted.

[For those of you who were not reading RISKS back in September, RISKS-1.6 had a lengthy piece by Al Friend on the CRT subject, plus some other comments in RISKS-1.5. However, Dan Hoey's query in RISKS-2.2 asked about a recent Swedish study. Apparently no one had seen it. PGN]

SRBs, What the Computers Should Monitor, and Expert Systems?

Jim Giles <jlg%a@LANL.ARPA>
Thu, 6 Feb 86 18:20:33 mst

In RISKS-2.5, Sean Malloy writes:
>One of the points that was brought up during the broadcasts the day of the
>disaster was that the telemetry tapes were going to have to be analyzed to
>determine if there was any indication as to what happened. The temperature
>data for the external tank was specifically mentioned as one of the
>telemetry streams that was NOT fed to a display in either the launch control
>area or Mission Control. The NASA spokesman explained that there was so much
>information coming in that a decision had to be made to limit what the
>launch control personnel had to pay attention to.

Has Expert System Technology been thought of as a fix for this problem? It would seem that a really fast computer (or several) could monitor all those inputs which aren't under the direction of human flight controllers and could be set to pop up warnings for any conditions that are unacceptably peculiar. The human flight controllers would still have the final word on what to do, the computer would just be there to watch those things that the staff normally can't. Are

expert systems yet advanced enough to make this worthwhile? If so,
are any being used?

In the Challenger case, there was a 4% loss of thrust in the SRB about 15 seconds before the explosion. If this had been correlated with a temperature rise in the ET or some other anomaly that indicated possible SRB burnthru, there might possible have been warning of the problem. An expert system might have been able to correlate several minor readings that together formed a pattern of SRB failure. A succinct display of the information together with the machine's conclusion could have been given to one of the controllers.

Of course, it is possible that the telemetry tapes contain no information that would have helped - even if it were monitored. Abort before the SRBs stop firing is (I'm told) a risky thing anyway, so advance warning may not have been of much value.

J. Giles
Los Alamos

<decwrl!decvax!cwruecmp!rexago1!rich@ucbvax.berkeley.edu>
Mon, 3 Feb 86 18:39:32 est

<K. Richard Magill>
To: decvax!risks
Subject: Redundancy in the Shuttle's Computers
Organization: Roadway Express, Akron, OH

>From: Mark S. Day <MDAY@XX.LCS.MIT.EDU>
>Subject: Redundancy in the Shuttle's Computers
>To: RISKS@SRI-CSL.ARPA

>A submission in RISKS-2.2 was concerned about a Stratus-like comparator
>mechanism being a single point of failure in the Space Shuttle's operations.
>However, the space shuttle's redundant set doesn't use a comparator
>mechanism. Instead, the actuators are controlled by a hydraulic
>"force-fight" mechanism, with each computer sending independent commands on
>independent buses. If one computer of four fails, the other three can exert
>enough force to overpower its (presumably bad) commands. If this pressure
>differential persists for long enough, the overpowered one is hydraulically
>bypassed.

How is a *single* hydraulic comparator any different than a digital "force-fight" mechanism?

K. Richard Magill
(don't know my address from arpa, maybe rexago1!rich%Case@csnet-relay
or rexago1!rich@case.csnet)

Nuclear Cargo in the Shuttle

<LShilkoff.ES@Xerox.COM>
Thu, 6 Feb 86 14:46 PST

An article in the L.A. Times of Feb. 6, 1986 discusses the dangers of
carrying nuclear cargo in the shuttle. The article states:

The Energy Department contends that the protective shell around the
plutonium would withstand explosive pressures up to 2,200 psi, and that
the shuttle explosion appears to be less than 2,200 psi. According to a
NASA-produced safety analysis report on the Galileo and Ulysses projects,
... a blast caused by activating the spacecraft's "command
destruct" mechanisms' explosive devices attached to the large external tank
and suspected of being detonated by Challenger's leaking solid rocket
booster would produce a burst of pressure ranging from 740 to 7,800 psi. If
a shuttle fails to get off the pad and topples over, even greater explosive
pressure could be generated...possibly as high as from 2,000 to 19,600 psi.

[By the way, this morning's SF Chron indicates the destruct charges
for the external tank were found intact. PGN]

Software Protection Symposium

<Barbara.Zayas%a.sei.cmu.edu@nrl-css>
Friday, 17 January 1986 13:41:46 EST

Software Protection Symposium
To Be Held in Pittsburgh 4-5 April 1986

PITTSBURGH -- "The Future of Software Protection", a two-day symposium
scheduled for 4-5 April 1986, will bring prominent legal scholars and others
together to discuss one of the most crucial and controversial legal issues
of the day. The symposium is jointly sponsored by the Software Engineering
Institute and the University of Pittsburgh Law Review. The program will
focus on intellectual property law and whether it can evolve to provide
adequate protection for software.

Topics to be discussed during the one and a half days include patent
protection for algorithms, simultaneous copyright/trade secret protection,
scope of fair use in copyright cases, ownership rights in computer generated
works, and sui generis protection for software without legislation.
Discussion on the second day will center on the Department of Defense's
software procurement policy.

The registration fee of $100 includes the University of Pittsburgh Law
Review issue in which articles by the major speakers will be published.
For further information, please contact Carol Biesecker, [412] 268-7786.

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 2: Issue 8

Friday, 7 Feb 1986

Contents

Expert systems and shuttles

<mlbrown@nswc-wo.ARPA>
Fri, 7 Feb 86 09:17:13 est

In Risks 2.7, J. Giles speculates:
>Has expert system technology been thought of as a fix for this problem?
>... a really fast computer ... could monitor all those inputs which aren't
>under the direction of human flight controllers...
>Are expert systems yet advanced enough to make this worthwhile?

Unfortunately, expert systems developed to handle such an occurrence would have to be based on a foreknowledge of the relationship of the various anomalies that occurred in the shuttle disaster. I seriously doubt that most competent systems safety engineers could have predicted the occurrence even with a full knowledge of the anomalies that occurred. Development of such an expert system would likely have to be based on that type of knowledge. However, expert systems aside, I am amazed that the NASA systems safety people would permit a multiple section rocket motor to be manufactured at one location and assembled at another. Misfortune has shown us in the past that these composite structure solid rockets have some very unique and undesirable properties. It will be interesting to see exactly where the failure occurred in the shuttle's SRB if in fact it did fail. If the failure occurred at some location other than the suspect joint, chalk another one up to experience.

Michael Brown

Expert systems to detect shuttle failure

Dave Platt <Dave-Platt%LADC@CISL-SERVICE-MULTICS.ARPA>
Fri, 07 Feb 86 10:11 PST

Well, it's certainly possible to set up some sort of expert system that would monitor incoming telemetry and issue warnings in case of possibly-dangerous combinations of unusual conditions. However, I can see a couple of difficulties involved here:

1- There are some conflicts re the amount of data that you want to feed into the expert-system tool. Certainly, the more data that is available (from many different classes of sensors), the smaller the chance that the tool won't have the information needed to detect the problem. [For example, Challenger was equipped with far fewer sensors on the SRB than was Columbia during its tryoug flights].

But... as you increase the number of individual sensors, and the amount of data (# of different classes of data, especially), you necessarily increase the number of rules in the system, and the amount of crunchpower necessary to step through the rules and determine whether any conclusions need to be brought to the attention of the controllers. It doesn't do you much good to receive a warning saying "Engine failure is probable, based on conditions xxx and yyy" if you don't get the warning in time to do anything about it.

In my [very limited] experience, very few if any existing expert systems are capable of handling large amounts of real-time data; the ones that I've seen tend to be somewhat sluggish. I don't doubt that it would be possible to build special-purpose hardware that would support such a system... but I don't believe it has been done yet.

2- As I understand them, expert systems are designed to reproduce (or mimic) the sort of what-if and maybe-then decision sequences that an expert would go through when analyzing a particular sort of problem. They work by encoding (in explicit form) the steps and conclusion that an expert would use. A large part of the work involved in developing an expert system is sitting down with the expert(s), and assisting them in encoding their (often implicit and unspoken) rules into rigorous form.

All well and good... BUT... the expert system's "expertise" is entirely limited by the completeness of the rules that are used to construct it. One cannot assume that an expert system will be able to detect or diagnose a situation that has never been encountered before... it may do so, if the rules were complete enough and if the situation is similar to one that has occurred before, but you don't want to bet your life on it!

Only the simplest expert systems can ever be considered to be "complete". When solving a complex, real-world problem (such as "Is the shuttle's current behavior normal?"), the best that you can expect is that some useful fraction of all possible situations will be analyzed in a meaningful fashion. Expert systems tend to grow and evolve as they are used... just as a human expert's capabilities do... and both humans and expert systems will tend to misdiagnose situations that fall outside of their current knowledge base.

3- Even if an expert system reacts quickly and accurately enough to give a meaningful warning ("SRBs leaking, ET overheating, explosion imminent"), you're still faced with: [A] Human reaction time (controller and pilot); [B] taking the necessary immediate action (split the SRBs from the ET and/or split the orbiter away from the ET); and [C] surviving (getting far enough away from the ET before it goes *BLOOIE*, and then completing a very difficult dead-stick turnaround and landing, or a tough water ditching). In the case of the Challenger explosion, it looks as if all three of these factors were dead-set against the crew... there was very little time to react, no way to get away, and a water ditching would probably have killed many of the crew.

I imagine that you could certainly build an expert system that would be capable of reading the shuttle's telemetry, and warning of most conditions THAT THE DESIGNERS OF THE SYSTEM HAD TAKEN INTO ACCOUNT! The real problem lie, of course, in detecting conditions that no one had expected would occur... if the system has no rules that would lead to a conclusion such as "The SRB segment ring seals are leaking", then the system will never report such a condition. At best, some other warning will be reported ("Asymmetric thrust from SRBs exceeding 2%"); at worst, no warning will be received, or the system will issue warnings unnecessarily ("Heavy engine vibration").

Plutonium

"MARTIN J. MOORE" <mooremj@eglin-vax>
0 0 00:00:00 CDT

I don't think the worries about plutonium should be dismissed out of hand. It is my understanding that the lethality of plutonium is due to its extreme toxicity, as opposed to its radioactivity. Comments from a knowledgeable chemist are eagerly solicited.

Re: Earthquake Monitoring Systems

Matt Bishop <mab@riacs.ARPA>
7 Feb 1986 1502-PST (Friday)

I took the liberty of forwarding Gary Leaven's question on earthquake monitoring systems (ie, are they designed to function during a major earthquake?) to Mike Raugh, the author of the CACM article which prompted the question. Here's his reply:

Matt,

The question you forwarded to me is a good one: Are the seismic instruments used in Calnet and the Southern California Array built to withstand the shaking of a major earthquake? The answer is Yes and No, but it doesn't matter! Even if a local subset of instruments (or the telemetry system serving that subset) is knocked out by a major quake, more distant instruments will pick up signals from the quake that will be adequate for locating, timing and calculating the earthquake "mechanism", i.e. direction of first motion, plane of rupture, magnitude. The purpose of the two arrays is to monitor earthquake activity throughout California, so you can see that the entire combined two arrays will almost certainly not be totally incapacited by a major quake, hence they will continue to monitor activity (even distant activity) successfully.

That being said, it should also be mentioned that seismologists are very interested in the fine-grained signals that are obtainable only at close range to a major earthquake (seismic waves that have traveled teleseismic distance through the earth lose much of the higher frequency energy). Such close-in data from large earthquakes can only be obtained from special "strong motion" instruments: this type of instrument furnished the data for Archuleta's study of the Imperial Valley quake discussed in my paper. Strong motion instruments are much more difficult to make, for all the obvious reasons, and are expensive compared to the ones that comprise the two arrays mentioned above.

The problem of designing sophisticated modern microcomputer based instruments that have sufficient sensitivity and dynamic range and are robust in the presence of violent shaking is a big one. Especially when you consider that such instruments must have local storage and power supplies to back up data collection in the event of telemetry break-downs. I can think of two groups at the USGS in Menlo Park that are working on systems of this kind. The first is lead by Roger Borchardt (his GEOS project was mentioned in my article). Another is being conducted by Larry Baker, Joe Fletcher, and Paul Spudich, who are developing a down-hole three-dimensional mesh of instruments for observation of the detailed progression of faulting expected to occur in the officially USGS-predicted earthquake at Parkfield. In other words, new designs for such instruments are on the frontier of research and development at the USGS. Very likely other work of similar import is taking place elsewhere.

I hope this answers your question.

Mike

Earthquake Monitoring Systems

<Murray.pa@Xerox.COM>
Fri, 7 Feb 86 03:13:43 PST

Neither of these stories involves mainline computer risks, but they might contribute some insight.

I got this story from a friend doing earthquake research for the USGS. I think it was '71 when a bigish quake near LA collapsed a VA hospital and a half constructed bridge. That generated a lot of interest in the way buildings (and bridges) react to quakes. Nobody really knew how much stress is present on various structural parts of a building. In response, many strain recording gizmos were installed in many large buildings.

Time passed, and everybody went back to their normal work. After several years, another bigish quake came along, and somebody remembered all those installed instruments. So they went out to collected them. Most of them had died. I don't remember any numbers, but I was left with the feeling that everybody was discouraged that they didn't get much interesting data.

Another friend worked on LASA (Large Area Seismic Array?). It was one of the early seismic arrays with hundreds of sensors scattered over eastern Montana. I think it was primarily part of the bomb test detection program. With that many sensors and that much wire and electronics to collect all the data, a few sensors were always off the air. They discovered that they got better data if they didn't tell the fixit crew that a test was coming.

Re: RISKS-2.7: Earthquake monitoring systems

Eugene Miya <eugene@AMES-NAS.ARPA>
7 Feb 1986 0849-PST (Friday)

... I can tell you that earthquake instrumentation really need not survive a local earthquake. Local measurement is very unreliable because of environmental factors: soil type, underlying geologic structures, and so forth

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 2: Issue 9

Sunday, 9 Feb 1986

Contents

Computerized train wreck? ... Computer-induced stock-market swings.

Martin Minow, DECtalk Engineering ML3-1/U47 223-9922 <minow%serf.DEC@decwrl.DEC.COM>
09-Feb-1986 2048

On the news recently, it was noted that the recent Canadian train wreck [8 Feb 1986] "shouldn't have happened as the system was computer controlled."

[Bill Dewan, spokesman for the Canadian National Railroad, was quoted in the SF Chron, 9 Feb 1986: "The [freight] train should not have left the double-track section, and whether its failure to stop was due to signal failure or human failure is what is under investigation." Death toll initially estimated 30 to 50. Eastbound transcontinental passenger train with up to 120 people aboard, head-on with westbound freight on single-track section, 75 yards after freight left double-track section. PGN]

In today's Boston Globe (Sunday, Feb. 9, 1986), an article by Rick Gladstone, Associated Press discussed problems caused by "the growing effect of computerized buying and selling programs that influence stock prices without regard to economic fundamentals that historically have shaped the market."

These programs monitor stock prices and future prices for the same stock, selling the stock and buying futures when the stock price exceeds the futures price and buying stocks and selling futures when the stock price falls below the futures price. "The investors, therefore, profit no matter what." ... The recent big swings of the Dow Jones average "are partly attributed by some Wall Street analysts" to these programs, "because they are activated at the same time and greatly increase the number of shares traded."

... Many analysts "agree that at least part of the Dow Jones industrial average's record 39.10-point plunge Jan. 8 was linked to a mass of sell-program orders activated by the computers."

Martin Minow minow%rex.dec@decwrl.arpa

Selectively Displaying Data -- Boeing 767 EFIS

Alan M. Marcum, Sun Consulting <sun!nescorna!marcum@ucbvax.berkeley.edu>
Fri, 7 Feb 86 16:17:06 PST

In Risks V2.7, Jim Giles raises a question regarding selective display of telemetry, with a computer helping control what is displayed. This is currently being done in the "Electronic Flight Instrument System" (EFIS) being used on, for example, the Boeing 767. The EFIS can be configured to display various data on command by the flight crew, and to display "flags" if certain things go outside the normal range. This is by no means using what we might consider full-blown expert systems technology.

For those unfamiliar with the 767 cockpit, or an EFIS in general, there are various CRTs under computer control. Usually, the tubes immediately in front of the pilot and the co-pilot display the flight attitude (an enhanced "artificial horizon"), often with airspeed, altitude, heading, and trends. Additional tubes display route and various engine parameters. These additional tubes are those used for displaying abnormal information.

A couple of EFIS configurations are available for some of the larger general aviation aircraft (for example, Beech's new Starship turboprop will be delivered with and EFIS). It is interesting in light of this digest to note that in all EFIS configurations I've seen, there are ALWAYS conventional (i.e. mechanical) backups for the critical instruments portrayed by the EFIS.

Cape Range Safety Display Systems

"LYNNE C MOORE" <moorel@eglin-vax>
0 0 00:00:00 CDT

Clive Dawson (in Risks 2.4) asked what kind of data display the Range Safety officer at Cape Canaveral uses to determine when to destroy missiles.

Data is collected from a wide variety of sources throughout the Eastern Test Range, including a number of radar and telemetry sites and optical trackers. The latter are especially important in the first few seconds of launch, when radars cannot be used due to multi-path problems associated with the large metal gantries. This data is collected by the Central real-time computers (redundant Cyber 740's), which determines the best and next-best estimates of present position and instantaneous impact point for the missile body. This is displayed by the Range Safety Display System (RSDS) computers along with plots of destruct lines, which indicate the limit of endangerment of a populated area if the missile's thrust were to terminate at that moment. These destruct limits are considerably broader on the Shuttle than they are for an unmanned missile. In addition, the RSO's maintain a voice link with the Shuttle Flight Dynamics Officer (in Houston), and they will not destroy the Shuttle as long as the crew is in control, even if the destruct line is violated.

The RSO's also have real-time telemetry displays and video plus a voice link to an observer as close to the launch pad as safety permits to assist at the initial moments of flight when the data is at its worst.

This system provides the best chance for crew survival within the limits of range safety, assuming there is enough time in a danger situation for crew response (which there wasn't in the Challenger explosion).

At the time that my husband, Martin Moore, was working on the destruct software at the Cape, I was working on a radar data switching system which is physically located in the same room as the RSDS system. I was also one of the near-real-time analysts for the Central computer, involved in reducing post-mission trajectory and orbital data. In the course of my duties, I learned a lot about the RSDS system and the other data collection/display systems at Cape Canaveral AFS (which is not quite the same thing as Kennedy Space Center -- KSC is NASA, CCAFS is the Air Force).

Lynne C. Moore (moorel@eglin-vax.arpa)

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 2: Issue 10

Wednesday, 12 Feb 1986

Contents

Computerized aircraft collision avoidance

Peter G. Neumann <Neumann@SRI-CSL.ARPA>
Wed 12 Feb 86 10:46:35-PST

As noted on various previous occasions, it is always nice to report computer-related successes in avoiding risks, but they seem to get scant notice. Perhaps some of you can keep your eyes open.

I had a phone report last night of a TV news item in Washington DC, relating to a computerized aircraft collision-avoidance system that succeeded in preventing what otherwise would have been a midair collision yesterday. Can anyone provide details?

Peter

Computerized Feedback and the Stock Market

<Nickell.pasa@Xerox.COM>
Mon, 10 Feb 86 08:31:17 PST

Martin Minow's note about the effect that computerized stock traders can have on the market brings up an interesting general situation.

Any self-correcting system which has a delay in the feedback loop (as opposed to something like a spring, where the feedback is instantaneous) can fail to correct itself if it is pushed too hard during a single feedback period. Further, if the forces acting on the system are themselves made a function of the system, there is the possibility of increasingly amplified oscillation until the system breaks down at some point.

The stock market is a case in point. Stock prices drift according to the buying and selling of the stock. But in the case Martin Minow cites, I am guessing that the computers were able to deluge the system with sell orders before the price could adjust itself.

The delay in price adjustment was not a problem until we had computers capable of swamping it with orders. Thus we may be introducing computers into environments where slowness provides some degree of stability to a process. Speed itself has its dangers.

Eric Nickell Nickell.pasa@Xerox.xcom

Analyst Changes City Treasurer's Computer Code

Mike McLaughlin <mikemcl@nrl-csr>
Mon, 10 Feb 86 10:14:01 est

D.C. FINANCE ANALYST LOCKED OUT OF OFFICE, GIVEN NEW DUTIES
Deputy Mayor's Employe Changed Computer
by Peter Perl, Washington Post Staff Writer

Plutonium on the Space Shuttle

415)486-5954]
Tue, 11 Feb 86 09:49:49 pst

Recent Freedom Of Information Act (FOIA) information has revealed that NASA officials considered the possibility of a Space Shuttle exploding to be so remote that the dangers of carrying tens of pounds of Plutonium aboard was not given much thought. Plans are apparently still in the works to launch these Plutonium driven space probes starting in May of this year. The manufacturer of these probes has claimed that the Plutonium element would have survived the Challenger explosion as material of similar strength was recovered from the debris.

Request to RISKS Readers from COMPASS 86 (COMPuter ASSurance)

Al Friend <friend@nrl-csr>
Tue, 11 Feb 86 10:41:50 est

WE NEED YOUR HELP

TO: The readers of the RISKS FORUM
FROM: Program Committee COMPASS 86

1. We need an estimate of attendees and authors at a conference we are planning. Also, we need input in terms of ideas and events for it.

2. The conference is COMPASS 86, which stands for COMPuter ASSurance.

This conference is all about the things we are discussing in this forum. The security and safety of processes rather than data banks, or communication links. We have in mind not only weapons and defense type systems, but medical systems, tranportation systems, and the multitude of computer controlled systems that touch our everyday lives.

Dave Parnas will be the keynote speaker.

There will be a series of panel discussions, which will address everything from SDI to the application of AI.

Papers will be reviewed by computer and software scientists working in the areas of safety and security from the University of California, SRI, and the Naval Research Laboratory.

The idea is to encourage new ideas, new applications of neglected ideas and promote useful interactions.

3. The conference specifics are:

DATE: 7-11 July 1986
PLACE: The George Washington University, Wash., DC
HONORARY CHAIRMAN (prospective): Ruth Davis, former Assistant to
Deputy Undersecretary of Defense
for Research and Advanced Technology
GENERAL CHAIRMAN (prospective): H.O. LUBBES, Space and Naval Warfare
Systems Command (lubbes@nrl-csr)
SPONSOR: IEEE Washington Section

4. It would help us if the readers of this forum could give us some feedback on the number of people likely to attend and the number of people likely to submit papers. Also, we would like to incorporate any special events that people would like to see into it. The important dates are:

```
    March 31 --- Abstracts Due
    April 30 --- Authors Notified
    May 30   --- Camera Ready Manuscripts Due
```

The call for papers is in the February issue of IEEE Computer. Also, a version of it ran a little while back in this forum.

[I won't comment on the risks of running the first conference of its kind! Good luck. 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 2: Issue 11

Sunday, 16 Feb 1986

Contents

SF Federal Reserve Bank 2 Billion Dollar Goof

Peter G. Neumann <Neumann@SRI-CSL.ARPA>
Sun 16 Feb 86 20:04:54-PST

The SF Chronicle (7 Feb 86) had an article on what was "perhaps the biggest banking blunder ever" (despite the Bank of New York just having had a $32 billion screw-up, reported in RISKS-1.31). On 21 January 1986, the Fed was testing its computers and accidentally transferred $2B to 19 financial institutions. A weekend test session had been constructed using 1000 actual transactions from the previous Friday. The test program and data were accidentally left around, and thus the transactions were repeated on Monday morning. As opposed to the $32B case, all of the money was recovered, and no actual losses were incurred. A spokesman "stressed, however, that $2 billion represents only 2 percent of the funds handled by the Fed each day." (... peanuts ... chicken-feed ...?) In the future, testing will be done with make-believe transactions and fictitious account numbers. Six employees deemed responsible were suspended without pay for three days.

[Thanks to W. Randolph Franklin <wrf@degas.berkeley.edu> for reminding me of that one. I had meant to include it earlier. PGN]

Washington D.C. Analyst's Password Game [more on RISKS-2.10]

the tty of Geoffrey S. Goodfellow <Geoff@SRI-CSL.ARPA>
15 Feb 1986 05:39-PST

a010 2248 14 Feb 86
PM-Password, Bjt,0580
Disgruntled Computer Analyst Asks D.C. Children To Solve Money Mystery
By DIANE DUSTON
Associated Press Writer

WASHINGTON (AP) - A disgruntled former District of Columbia employee who hid the code word to computerized city accounts is inviting children to try to find the password by playing a game he is placing in a newspaper.

Alvin C. Frost, an accountant for the city, said Friday he would have clues published in The Washington Post this Sunday to a code word he used to hide accounts in the city's computer system.

The game is the latest twist in an ongoing dispute between the district and Frost, who hid the accounts because of what he says are mismanagement and improprieties in the city's finance office. He has not accused officials of criminal wrongdoing.

Frost, who worked for the city's office of financial management 3 1/2 years, resigned Friday.

The accountant is asking children 12 years old and under to guess the password based on the clues and win a tour of the monuments, White House, Capitol, and Supreme Court and lunch in a downtown restaurant.

''Kids like to be involved in what is going on in the news,'' Frost said. ''Maybe this little game will get people involved in what's going on.''

Though city officials say computer experts helped them crack the code and regain access to the hidden accounts, Frost said he doesn't think they know the password he used.

''Right now, they don't know. They don't know what's in the computer,'' said Frost, who says he designed the computer program used to manage the city's cash.

Frost said there may be a ''tapeworm,'' or malfunction, in the city's computer that could consume files if the word is not discovered.

''I planted the seed (to such a malfunction). Whether it actually exists, they'll have to find out,'' said Frost.

He was stripped of all his responsibilities after he devised the new code word and refused to tell his superiors.

He said he was resigning effective March 15, ''for historical and literary reasons,'' a reference, he said, to the Ides of March, when Julius Caesar was assassinated by a group of trusted friends.

''I've done my job,'' said Frost. ''Now it is time for the people to get involved.''

Frost gave reporters a chance to figure out the password by offering these clues:

-It has seven characters.
-It has two syllables.
-It's a real word.
-All the characters are letters.
-The word is not in the Declaration of Independence.
-But the first syllable is used four times in the Declaration.
-And, it is what the Declaration really means.

At the news conference, a reporter guessed ''freedom,'' but Frost wouldn't confirm it as the password.

Officials did not return phone calls seeking comment Friday after Frost announced he would resign.

He said that last October he was questioned by the FBI and IRS about operations in the office. He said the IRS was ''looking to trace the trail of possible payoffs,'' but he would give no further details.

Frost changed the password to some computer accounts after someone entered the system and made copies of a letter he had written to Mayor Marion Barry Jr. with his complaints.

He was stripped of his responsibilities, though not fired, when he refused to tell his superiors the code word.

AP-NY-02-15-86 0147EST

Re: Boeing 767 EFIS -- compare Airbus A320

Rob Warnock <sun!redwood.uucp!rpw3@ucbvax.berkeley.edu>
Fri, 14 Feb 86 02:53:46 PST

Alan Marcum <marcum@sun.uucp> writes:

```
+---------------
| ...currently being done in the "Electronic Flight Instrument System" (EFIS)
| being used on, for example, the Boeing 767.  The EFIS can be configured to
| display various data on command by the flight crew, and to display "flags"...
|                       ... It is interesting in light of this digest to note
| that in all EFIS configurations I've seen, there are ALWAYS conventional
| (i.e. mechanical) backups for the critical instruments portrayed by the EFIS.
+---------------
```

Well... see pages 14-17 of the special supplement on Keyboards & Switches in Electronic News, Monday, February 10. These four pages have a special on the new style cockpit showing up on recent planes, and has a very nice color picture of the A320 cockpit. The Airbus A320 has no conventional yoke to fly the plane with -- each pilot has only a small "side stick", much like the shuttle pilots. Quote: "The side sticks are used to apply the input order such as azimuth and climb angle while the on-board computers take complete responsibility for applying the correct amount of power and for leveling off the aircraft at the desired altitude. An A320 aircraft cannot be commanded to go into an overspeed, overload, or stall condition..."

I commend the entire article to the readership of this list, since it has other little goodies in it, like: "When operation is normal, the flight deck is a dark and restful place. When an event happens that needs a pilot's attention, lights go on, displays change color. Formerly, when this happened, pilots had to make decision, throw switches. They had to really take charge. Now, although there are noticeably fewer switches for the pilot to get involved with, the switching still goes on behind the scenes, as systems and circuits test themselves and make decisions that call for no human intervention... And the over-riding benefit is the avoidance of human error."

I'm sure the decrease in display density helps an awful lot. But what happens

when a pilot is trying to analyze a critical display and it changes on him/her
because the system thought a new display was more important? Maybe the system
was right. We'll see...

Oh yes, they saved enough money on switches and instruments to go from
doubly-redundant to triply-redundant computers. That's nice... ;-}

p.s. Not knocking it, you know, just noting that pure fly-by-wire is
already here, including ordering the plane "to navigate to a selected
airport and make an unassisted landing."

Rob Warnock
Systems Architecture Consultant

UUCP: {{ihnp4,hplabs,dual}!fortune,sun,ism780c}!redwood!rpw3
DDD: (415)572-2607
USPS: 627 26th Ave, San Mateo, CA 94403

Networks Pose New Threats to Data Security [InfoWorld-86/2/10]

Werner Uhrig <CMP.WERNER@R20.UTEXAS.EDU>
Thu 13 Feb 86 04:32:42-CST

> "As local area networks become more commonplace in the corporate computing environment, the possibility of prying eyes gaining access to your data is significantly increased. And the spy is likely to be someone who knows you well."

[nothing earth-shaking or new, just interesting to see what issues the
"popular press" pulled into the spotlight.]

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 2: Issue 12

Tuesday, 18 Feb 1986

Contents

Risks in automobile microprocessors -- Mercedes 500SE

Peter G. Neumann <Neumann@SRI-CSL.ARPA>
Tue 18 Feb 86 20:28:05-PST

We have had the El Dorado brake microprocessor recall, the Mark VII computerized air suspension recall, and the on-going CB interference problem in automotive microprocessors. For the record, let me add the current manslaughter trial of John C. (Sandy) Walker, who was driving when his 1982 Mercedes 500SE went into an uncontrollable skid. He escaped, but his passenger was killed in the resulting flames. An "accident reconstruction specialist", Paul O'Shea (also a consulting engineer for Mercedes and NASA, and winner of three championship races), testified that the state-of-the-art anti-skid braking system malfunctioned. When working properly, it is designed to slow the vehicle gracefully, and "will leave no skid marks, no matter how hard you step on the brakes." The longest skid marks from the accident on 9 June 1984 on the Silverado Trail in the Napa Valley were measured at 368 feet! One line of investigation is that mechanical defects

might have caused a fire in the engine compartment, resulting in the malfunction of the brake computer. O'Shea noted that the emission-control system had been fitted with rubber hoses where metal hoses should have been, and which were placed too close to a heat-producing exhaust header.
[SF Chronicle 5 Feb 86]

Train safeguards defeated

<Chuck.Weinstock@a.sei.cmu.edu>
Tuesday, 18 February 1986 15:49:12 EST

You will recall the recent head-on collision between a Via passenger train and a freight in Canada [Risks-2.9]. A recent series of relevant messages on the railroad discussion list follows. For background, note that the Burlington Northern Railroad has had a significant number of "cornfield meets" (railroad slang for train collisions) in the past few years. Many were later blamed on alcohol and drugs being used by the crew. (It has gotten so bad that when the BN notified the community that it would transport no steam locomotives over it's most reasonable route to Vancouver for the Expo there, many railfans breathed a sigh of relief...they wouldn't want to trust something as precious as a steam locomotive to a railroad with a history of collisions.)

Chuck
- - - - Begin forwarded message - - - - [...]
From: FarleighSE <sef@drutx.uucp.arpa>
Subject: Re: VIA rail train collides head-on with freight.
Date: 13 Feb 86 23:16:16 GMT
To: railroad@rochester.arpa

>Engines have "dead-man" controls. I know that the E- and F-unit diesels
>had foot pedals that the engineer had to keep depressed continuously.
>If the engineer let up on the pedal, emergency brakes would be applied.
>I'm not sure the pedal system is in use today, but some variation is.
>On GO Transit in your neck of the woods, for example, the engineer has
>to be in contact with some part of the controls regularly (the throttle
>or brake lever, for example). If he/she hasn't touched the controls
>for 30 seconds, an alarm buzzes in the cab, telling him/her to touch the
>controls at least briefly to confirm that he/she is still alive. If
>no contact is made, on go the brakes!
>
>Carl Blesch

Burlington Northern removed their Deadman controls a number of years ago. It seems that the Engineers were overriding the system (putting a brick on the pedal?). So the management of BN (means Better'n Nothin') decided to remove the Deadmans throttle altogether. About two years ago one of the many BN wrecks could have been avoided if the Deadman's throttle was installed and used. It seems that instead of BN's management addressing the problem of their many times stoned crew defeating the saftey device they opted to remove the safety device.

Scott E. Farleigh
AT&TIS

- - - - End forwarded message - - - -

Security Safeguards for Air Force Computer Systems

Dave Platt <Dave-Platt%LADC@CISL-SERVICE-MULTICS.ARPA>
Tue, 18 Feb 86 12:31 PST

From the Los Angeles Times, 2/17/86:

"WASHINGTON (UPI) - The Air Force has failed to properly safeguard 77% of its computer systems, allowing the possible breach of classified data on space boosters, 'Star Wars' technology and major weapons systems, Pentagon auditors and officials say.

The security vulnerability also extends to sensitive data on the MX and Midgetman missiles and B-1 and F-16 aircraft, they say.

An Air Force official, responding to queries about the disclosure, said that he was '95% confident' that no 'actual compromises' of classified information on computers had actually occurred.

The Air Force Audit Agency, which inspected eight bases, sharply criticized officers at each facility for failure to inspect safeguards, such as lead boxes designed to limit electromagnetic signals emitted by the equipment..."

How can Alvin Frost fight City Hall?

Jim DeLaHunt <JDLH@SU-SUSHI.ARPA>
Mon 17 Feb 86 18:22:01-PST

I am intrigued by the apparent success of analyst Alvin Frost's attempt to keep the city of Washington, DC out of their own computer. With one 7-character password (and apparently physical access to the machine) he seems to be able to keep certain files out of the reach of his superiors. Does anybody know:

* What machine, OS, etc. this is?
* Whether his superiors have in fact cracked his protection?
* What sort of data protection systems are immune to a legitimate systems manager logging on as root (or OPERATOR or whatever)?
* What is actually going on here?

Send responses to me; I will be glad to summarise to the net.
--Jim DeLaHunt, Stanford University JDLH @ SU-Sushi.ARPA

More Plutonium/Shuttle

"MARTIN J. MOORE" <mooremj@eglin-vax>
0 0 00:00:00 CDT

The 2/17/86 issue of Aviation Week contains an article entitled "Officials Disagree on Data Assessing Shuttle Reliability." The main topic of the article is the danger of plutonium contamination from nuclear shuttle payloads in case of an accident (I seem to have heard about this somewhere before :-). I recommend the article to the RISKS readership. One quote from Robert K. Weatherwax, author of a study titled "Review of Shuttle/Centaur Failure Probability Estimates for Space Nuclear Mission Applications" [December 1983] seems to answer the questions we were throwing around:

> We concluded that many, if not most, solid rocket motor failures would result in some release of plutonium, or at least a high likelihood of that. We recommended more safety analyses be done to evaluate the likelihood of booster failures in conjunction with this nuclear risk.
> A nuclear payload cannot explode, but it can be broken up, vaporzied or fragmented. You would have prompt fatalities on the ground and substantial contamination in eastern Florida [if a catastrophic launch failure occurred.] In a worst possible case, you could double the entire worldwide burden of plutonium in the atmosphere.

Weatherwax is head of Sierra Energy and Risk Assessment, located in Sacramento. Sierra was contracted by the Air Force to perform the study.

[BERLIN: Computerized Voting]

"Steven A. Swernofsky" <SASW@MC.LCS.MIT.EDU>
Tue, 18 Feb 86 23:06:33 EST

...
Date: Tue 18 Feb 86 13:51:03-EST
From: Steve Berlin <BERLIN@XX.LCS.MIT.EDU>
Subject: Computerized Voting
To: bboard@XX.LCS.MIT.EDU

Wednesday, February 19, 1986, 7:30

Ms. Eva Waskell

Independent Investigative Reporter and Science Writer

``Computerized Voting: No Standards and a Lot of Questions''

Ms. Waskell will address problems involved with computerized voting programs. She will relate the status of litigation in several jurisdictions and will suggest safeguards in the voting system.

Ms. Waskell's research provided a basis for several New York Times articles exposing problems with the most popular computerized balloting system in use.

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 Steve Berlin at 617-253-6018.

◀ ▲ ▶ ⓘ

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 2: Issue 13

Thursday, 20 Feb 1986

Contents

Dec. 8 cruise missile failure caused by procedural problems

"MARTIN J. MOORE" <mooremj@eglin-vax>
0 0 00:00:00 CDT

Last December 8, a Tomahawk cruise missile was launched from a submarine in the Gulf of Mexico. It was intended to fly around southern Alabama and the Florida panhandle and then crash onto the Eglin AFB reservation; however, about 9 minutes into the flight the missile made a sudden right turn and crashed outside the reservation near the small town of Freeport (the residents of Freeport were less than amused.) No explanation for the failure was given until an article in the 2/20 issue of the "Playground Daily News" [Fort Walton Beach, Florida]. The article says in part:

> Human error caused a malfunction that led to the errant flight and subsequent grounding near Freeport of an unarmed cruise missile on a test flight two months ago...Newly released information shows that a "procedural problem" involving the missile's computer guidance system caused the malfunction [according to a Navy spokesman]...He said the middle portion of a launch-fly-recovery program guidng the sophisticated

missile was erased when the launch crew loaded the information into the
missile's memory banks too quickly. As a result, the missile went from
the launch mode straight to the recovery mode "without going through the
most important part of the mission"..."That's what caused it to make the
unscheduled turn," he said. "It was not the missile's fault. It did
exactly what it was supposed to do."..."It was not a mistake. In reviewing
the procedures we can see how it happened. Since then, new directions and
new procedures have been instituted."

Old saying: If all else fails, follow the instructions.
New corollary: If you follow the instructions, you can't make a mistake.
(or, "I was only following orders, Your Honor.")

Computerized voting

Matt Bishop <mab@riacs.ARPA>
19 Feb 1986 0804-PST (Wednesday)

Unfortunately, I'm not in Massachusetts, so I won't be going to Ms. Waskell's lecture on computerized voting. But ever since I heard about the electronic tally board in some legislative house (I think the U.S. House of Representatives), I've been interested in the safeguards. The method used involved the legislators pushing one of two buttons at their desk (one for "yea", the other for "nay"). Well, it seems that some legislators pushed buttons for colleagues who were absent and who did not know how they were "voting"!

Now, this story may be apocryphal (since I don't remember the source, you might as well take it with a grain of salt) but it does bring up a point I've not heard addressed. If you use an electronic "ballot puncher" (as opposed to manually punching the cards then counting them electronically) how can you ensure the ballot is punched correctly?

So, my questions to this group: Anybody know if all electronic voting schemes used at election time require manually punched ballots? If not, what tests are the electronic "ballot punchers" subjected to in order to test their reliability? (I gather there can be no precautions against someone voting for someone else other than careful checks at the precinct, by the precinct workers. Opposing comments welcome!)

Non-science quotations on Plutonium (Risks 2.12)

Ayers.PA@Xerox.COM <Bob Ayers>
19 Feb 86 11:00:20 PST (Wednesday)

From Risks 2.12:
"In a worst possible case, you could double the entire worldwide
burden of plutonium in the atmosphere."
Robert K. Weatherwax, head of Sierra Energy and Risk Assessment

I find this quotation silly and non-science. Here are two meanings for his sentence:

1. The accident could double the instantaneous weight of Pu in the atmosphere.

   So what? Weatherwax supplies no figure for the current atmosphereic Pu burden, and no figure for that burden's harm or risk.
   Anyone know what the current level of Pu is? If its one femtogram, or even one milligram, who cares what "doubling" it does?

2. The accident could double the amount of Pu that has been added to the atmosphere by man.

   That's probably what Weatherwax wants you to read into his sentence. And its clearly silly, because when an above-ground Pu atom bomb goes off, MOST of the 10-20 kilogram critical mass of Pu goes into the atmosphere. Considering the number of above-ground bombs tested, this would mean that the "accident" involved at least a tonne of Pu!

Look at the loaded words: "double" "entire" "worldwide". Would his sentence have changed meaning if he had simply left out the words "entire worldwide"? No, but it wouldn't have sounded like a drum-roll was being played in the background. This isn't science, guys, this is politics -- or silliness.

[If we horse around a little, we might get to Whinny the Pu. PGN]

Software Piracy

D.Reuben <S.D-REUBEN@KLA.WESLYN>
Thu 20 Feb 86 16:34:11-EST

In Risks-2.11, I noticed that it was suggested that one way that software manufacturers combated software piracy was by providing various "extras" with their software packages which supposedly enhance the value of the product. To an extent, this is true, and I will grant that those who are really interested in a said game (business software is another matter) will purchase it rather than copy it because of the extras and the value that they provide during the playing of the game. However, I submit that the vast majority of computer users are only casually interested in a certain "new game", and because of this will not be too deterred by the lack of colorful maps or cute little clues which are provided with the game. These can easily be described or listed in a small and easily written text file, and distributed all over the US and Canada with the actual "cracked" game that is being pirated. Thus, these objects included with the software are only a deterrent for the interested player, who probably buys most of his software anyhow. Software companies do not loose money due to these people, rather, it is the software trader who seeks to get new software at a regular rate (which with a modem is exceptionally easy to do) who is the main threat to software company profits, and large cloth maps and parchment instructions thrown in to the software package are of little interest to some one who can easily get the complete instructions and contents of the "extras" all typed up in a neat little text file. This also goes for games like "Captain Goodnight", which sought to deter piracy by having a set of codes, which if not used properly in various sections of the game, would cause the program disk to reboot (Apple version). However, it was just as easy to type up the chart that the software manufacturer provided and include it with the program on the same disk. Versions have even been circulated where the section of the program that asks for your 'ID code' is taken out, and the game proceeded as if the user had typed in the right code.

One further thing - Another notable software manufacturer which is reputed for their software protection policy is Beagle Brothers, who provide valuable utilities and some games for the Apple which are unprotected and at a much more modest cost then most of its competition.

D.Reuben   Reuben@Weslyn.Bitnet (or Reuben@Weslyn.Arpa)

Air Force Security Safeguards (RISKS-2.12)

Stephen Wolff <steve@BRL.ARPA>
Wed, 19 Feb 86 4:10:21 EST

> Subject: Security Safeguards for Air Force Computer Systems
> "WASHINGTON (UPI) - . . . .
>
>   The Air Force Audit Agency, which inspected eight bases, sharply
> criticized officers at each facility for failure to inspect safeguards,
> such as lead boxes designed to limit electromagnetic signals emitted
> by the equipment..."

Bet the spells to ward off evil spirits weren't current, either.

[If you think that Steve's remark is off the
mark for the RISKS Forum, you could be wrong.
But no spirited follow-ups, please. PGN]

Shuttle Safety

Peter G. Neumann <Neumann@SRI-CSL.ARPA>
Thu 20 Feb 86 16:51:02-PST

EXCERPTED FROM THE BBOARDS:
c.1986 N.Y. Times News Service: news summary for Thursday, February 20, 1986

Washington - NASA's technical experts reviewed the shuttles' booster rocket sealing problems last August without considering the impact of cold weather on the seals or giving much attention to the possibility that launchings should be delayed while the seals were strengthened, according to a key participant in the top-level review and recently released documents. The participant, William H. Hamby, deputy director of shuttle program integration, described in an interview a history of rising concern over the rocket seals.

New York - Shuttle safety margins were cut to adhere to an accelerating launching schedule, according to space agency documents made public by the chairman of a House panel. The chairman, Rep. Edward J. Markey, D-Mass., said the actions, coupled with the explosion of the Challenger, raised basic questions about the safety of the shuttle design and precautions by the space agency.

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 2: Issue 14

Monday, 24 Feb 1986

Contents

Automotive Problems Intensify

Peter G. Neumann <Neumann@SRI-CSL.ARPA>
Mon 24 Feb 86 11:20:54-PST

The National Highway Trafic Safety Administration has expanded its investigation into the sudden acceleration of automobiles to include vehicles made by six manufacturers. The expanded inquiry involves 1.4 milion mid-size and full-size cars made by Ford Motor Co (1984-85 model years), 100,000 Audit model 5000 cars (1984-85), 350,000 280Z and 380Z Nissan cars (1980-85), 400,000 Alliance and Encore cars made for American Motors-Renault (1983-85), and 140,000 Toyota Cressida luxury cars (1981-84). [See today's NY Times, SF Chron, etc.]

We have reported here previously on effects of radio-frequency interference on automobile microprocessors (e.g., RISK-1.23 and 24). This sounds like lots more of the same. Is the same chip-set involved, or is this a new kind of common-mode fault across different chip manufacturers?

Peter

A hard rain is gonna fall (around March 23)

"MARTIN J. MOORE" <mooremj@eglin-vax>
0 0 00:00:00 CDT

According to "Das Bild", a West German newspaper, a Soviet spy satellite has lost its steering capability and will impact between March 21 and March 25. Cosmos 1714, launched December 28, is presumably powered by an atomic power plant. The Soviets have not (as far as I know) commented on this yet.

misdirected modems

<hp-sdd!hpfcla!ajs@nosc.ARPA>
Mon, 24 Feb 86 11:12:54 pst

Twice recently, computers at our company (Hewlett-Packard) have been the embarrassing causes of telephonic annoyance. Phone numbers entered incorrectly in uucp L.sys files, due to typos or misunderstandings, have led to systems repeatedly calling private telephones in Fort Collins. The recipients of such calls, understandably annoyed, have had to backtrack through Mountain Bell to discover the cause.

I bet this happens a lot more than anyone realizes or admits.

Alan Silverstein, Hewlett-Packard Fort Collins Systems Division, Colorado
{ihnp4 | hplabs}!hpfcla!ajs, 303-226-3800 x3053, N 40 31'31" W 105 00'43"

Witch hunts, or Where does the buck stop?

<mlbrown@nswc-wo.ARPA>
Fri, 21 Feb 86 08:38:21 est

I note with interest that we have yet to hear from anyone who performed system safety analyses on the solid rocket booster system. Where are the system safety engineers who analyzed this design?

Spells and Spirits

Steve Berlin <BERLIN@XX.LCS.MIT.EDU>
Fri 21 Feb 86 11:31:55-EST

The comment about spells and spirits in the RISKS 2.13 reminded me of a set of papers from Princeton that readers of this forum might be interested in.

First, the references:

"The Persistent Paradox of Psychic Phenomena: An Engineering Perspective"
Robert G. Jahn, Proceedings of the IEEE, Vol 70, No. 2, Feb. 1982

"Princeton Engineering Anomalies Research"
R.G. Jahn, B.J. Dunne, and R.D. Nelson, technical note PEAR 84002

"An REG Experiment with Large Data Base Capability, III: Operator
Related Anamolies"
R.D. Nelson, B.J. Dunne, R.G. Jahn, technical note PEAR 84003

All three papers describe experiments in which humans attempt to influence the distribution of random events using 'psychic' means. According to the authors, the results indicate that there ARE deviations that range in likelihood from 10^-4 to 10^-7. I will not attempt to summarize any further, interested readers should contact the authors directly at:

Princeton Engineering Anomalies Research
School of Engineering/ Applied Science
Princeton University
Princeton, NJ 08544

I would like to type in the abstracts, however, the latter two papers explicitly "withhold the right to reprint or quotation".

The abstract for the IEEE paper follows:

Although a variety of so-called psychic phenomena have attracted man's attention throughout recorded history, organized scholarly effort to comprehed such effects is just one century old, and systematic academic research roughly half that age. Over recent years, a sizeable spectrum of evidence has been brought forth from reputable laboratories in several disciplines to suggest that at times himan consciousness can acquire information inaccessible by any known physical mechanism (ESP), and can influence the behavior of physical systems or processes (PK), but even the most rigorous and sophisticated of these studies display a characteristic dilemma: The experimental results are rarely replicable in the strict scientific sense, but the anomalous yields are well beyond chance expectations and a number of common features thread through the broad range of reported effects. Various attempts at theoretical modeling have so far shown little functional value in explicating experimental results, but have served to stimulate fundamental re-examination of the role of consciousness in the determination of physical reality. Further careful study of this formidable field seems justified, but only within the context of very well conceived and technically impeccable experiments of large data-base capability, with disciplined attention to the pertinent aesthetic factors, and with more constructive involvement of the critical community.

Disclaimer: I don't currently hold an opinion on the validity of the experiments described in these papers. I do, however, agree that there are phenomena which 'modern science' has no satisfactory explanation.

-- Steve

[I don't expect that RISKS will go lurching off in this direction. But, nevertheless, there is certainly a wide collection of issues related to risks to the public in the use of computer systems. An intriguing bit of science fiction along that line is the old novel by Ingo Swann, Star Fires. 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 2: Issue 15

Tuesday, 25 Feb 1986

Contents

Software Safety Survey

Nancy Leveson <nancy@ICSD.UCI.EDU>
22 Feb 86 12:20:49 PST (Sat)

I have been interested in safety for the past five years and have just completed a long-term project to write a survey of software safety. It includes sections on whether there is a problem (probably not of doubt to those who already read RISKS), why there is a problem, the implications for software engineering research, the relationship of software safety to software reliability and security research, a definition of software safety, a brief survey of relevant aspects of system safety, and a description of software safety techniques and research issues (requirements analysis, verification and validation of safety, assessment, software design, and human factors). Although good software engineering techniques will undoubtedly add to the safety of software, this is not a software engineering survey -- emphasis is on needed additions and changes to current software engineering techniques and research and on new procedures which have special relevance to safety. It is also a technical rather than a political document (although a few ethical and political issues are mentioned in the conclusions).

The paper is currently in the form of a technical report although it has been submitted to Computing Surveys (chosen primarily because of the size of the document -- about 60 pages). I will be glad to send out a reasonable number of copies in exchange for any comments which might help me to improve it. Comments on what you like and think is correct or helpful would be nice along with the complaints. If you would like a copy, send your regular mail address (not e-mail) to me: nancy@uci.edu (after March 4 my e-mail address is changing to nancy@ics.uci.edu).

Nancy Leveson
ICS Dept.
University of California, Irvine

Titanic Effect

Nancy Leveson <nancy@ICSD.UCI.EDU>
22 Feb 86 12:21:30 PST (Sat)

In Peter Neumann's latest SEN column, he mentions the Titanic Effect without an explanation of why it occurs.

[Actually, JAN Lee introduced it unattributably in RISKS-1.21:
The severity with which a system fails is directly proportional
to the intensity of the designer's belief that it cannot. PGN]

I would like to suggest a hypothesis. The Titanic effect is essentially the statement that the worst accidents often occur in systems which are thought to be completely safe. The Titanic was thought to be so safe that normal safety procedures, such as having an adequate number of lifeboats, were neglected with the result that many more lives were lost than might have been necessary.

The lesson is an important one because it goes back to the problems of using quantitative assessment techniques. Quantitative risk assessment can provide insight and understanding and allow comparison of alternatives. Probabilistic approaches have merit in that the necessity to calculate very low probability numbers forces on the analyst a discipline that requires studying the system in great detail. But there is also the danger of placing implicit belief in the accuracy of a calculated number. That is, it is easy to place too much emphasis on the models and forget the many assumptions which are implied. The models can also never capture all the factors, such as quality of life, that are important in a problem. (see Morgan -- Probing the Question of Technology-Induced Risk, IEEE Spectrum, Nov. 1981).

Getting back to the Titanic, certain assumptions were made in the analysis that did not hold in practice. For example, the ship was built to stay afloat if four or less of the sixteen water-tight compartments (spaces below the waterline) were flooded. Previously, there had never been an incident where more than four compartments of a ship were damaged so this assumption was considered reasonable. Unfortunately, the iceberg ruptured five spaces. It can be argued that the assumptions were the best possible given the state of knowledge at that time. The mistake was in placing too much faith in the assumptions and the models and not taking measures in case they were incorrect (like the added cost of putting on-board an adequate number of lifeboats). The Titanic is not an isolated example. Safety devices (such as sensors in solid-rocket boosters or software safety analysis and design procedures) cost -- usually in terms of dollars and performance. There are often attempts to get around them by using models which show that the hazards are so negligible that the cost is unjustified. On the other hand, too much safety can make the system unusable or unprofitable which is not the answer either.

The Titanic provides an important lesson for us involved in building safety-critical computer systems. Our current models for software reliability make a large number of assumptions which may be unrealistic or just not hold for particular systems. This is true also, to a lesser extent, with the hardware reliability models. Much effort is frequently diverted to proving theoretically that a system meets a stipulated level of risk when the effort could much more profitably be applied to eliminating, minimizing, and controlling hazards. I have seen a great deal of effort spent on trying to prove that a system which contains software has two or three more "9's" after the decimal point in the reliability models when the effort and resources might have been more effective if applied to using sophisticated software engineering and software safety techniques.

Nancy Leveson
ICS Dept.
University of California, Irvine

F-18 spin accident

<ihnp4!utzoo!henry@seismo.CSS.GOV>
Tue, 25 Feb 86 02:44:45 EST

Recent reading of a book on the F-18 turned up a couple of details on the spin accident that might be of interest; I don't think these were part of the original reports.

(For those who haven't heard about this before... The US Navy's F-18 fighter is heavily computerized, including "fly by wire" controls in which the computers always mediate between the pilot's controls and the aircraft. One thing the software does is to limit control-surface movements to within safe ranges, so the pilot cannot accidentally break the aircraft in combat maneuvering. The 12th prototype was lost when it got into a peculiar type of spin and the software did not give the pilot enough control authority for recovery. The pilot ejected safely. After investigation, the software was modified.)

Detail number one has something to say about the problems of exhaustive testing: even after the problem was known to exist, it took 110 attempts to duplicate the spin!

Detail number two is that the spin was *not* unrecoverable. The spin-test F-18 was equipped with an anti-spin chute just in case, but the pilot who first duplicated the spin discovered that he could recover without the chute by setting the outer-side engine to flight idle and the inner-side engine to full afterburner. The original pilot could have done this, had he thought of it. This might strengthen the case for giving flight-control software more authority, so that such unorthodox substitutes for ineffective or damaged controls could be employed automatically.

Reference: Bill Gunston, "F/A-18 Hornet", Ian Allan 1985, p. 43. Gunston does comment that apart from this one strange spin mode, the F-18 is probably the most spin-proof fighter in existence.

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

Re: Space shuttle problems (a comment on risks in general)

Brad Davis <b-davis@utah-cs.arpa>
Mon, 24 Feb 86 19:53:39 MST

If the current speculation about the shuttle is true (that seals on the solid fuel rockets failed because of the cold and that the Thiokol engineers asked for a delay because of their worries) then we should look more at the humans in any decision chain. Most of the major failures that I can recall were due to humans overriding the expert system (whether it was a electronic, mechanical, or human expert system) or just messing things up in the first place (like the UPL power generator that was connected to the power grid backwards, made a real big electric motor for a short time).

Brad Davis {ihnp4, decvax, seismo}!utah-cs!b-davis
b-davis@utah-cs.ARPA
One drunk driver can ruin your whole day.

Re: Misdirected modems

Matt Bishop <mab@riacs.ARPA>
24 Feb 1986 2221-PST (Monday)

Reminds me of something I read at 7 SOSP. Someone got the bright idea of collecting computer horror stories (an excellent idea, by the way!) and one of them involved one computer calling another. The connection suddenly quit working after about a year. The system people got curious and hooked an audio device to the telephone line. They then told the computer to contact its counterpart. They heard the computer dial, the phone at the other end go off hook, and the computer send its whistling tones indicating it had something to say. From the other end came the words, "Martha, it's that nut with the whistle again."
Problem solved.

Matt

[Thanks for the anonymous plug. It was I who anthologized the
anecdotes for 7 SOSP, and they all appeared in ACM Software
Engineering Notes Vol 5 no 1 (January 1980) -- as noted at the
very bottom of my disaster list in RISKS-2.1! PGN

◀ ▲ ▶ ℹ ✎ **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 2: Issue 16

Tuesday, 25 Feb 1986

Contents

---

volunteers to study security of computerized voting booths?

Kurt Hyde DTN 264-7759 MKO1-2/E02 <hyde%topcat.DEC@decwrl.DEC.COM>
Tuesday, 25 Feb 1986 04:45:16-PST

How secure are computerized voting booths?

I teach Systems Analysis at a local college here in Nashua, NH. For the last two years, my students and I have been studying the impact of computerization on voting security. The recent charges of fraud in Mexican and Phillipine elections increase the importance of such studies as computers are now being implemented into three areas of voting -- maintaining voter registration lists, tallying of votes, and directly computerized voting.

Last year's class discovered that an OEM was manufacturing a computerized voting booth. Further research has revealed that the company's strategy for ensuring security is secrecy of operation. Secrecy of operation increases the difficultly in penetration, but it also has a negative side effect of making it difficult (if not impossible) to detect tampering.

There are many documented cases of accidental miscalculation in computerized vote tallying equipment. The reasons why such errors were discovered is because reconstruction and recount was possible. Investigators reconstructed by gathering the machine-readable ballots. They were then able to recount by machine or by hand. Such reconstruction is impossible with the current state of the art in computerized voting booths because no physical ballots are created. Recounts in such cases are wholly dependent upon the software to have stored each vote in its proper storage location at the time of voting.

As far as I can tell, no computerized voting booth has ever been subjected to product testing by hackers. I discussed this with the chief engineer at the first company to make computerized voting booths. He agreed with me in a phone conversation that such testing would be nice and that he was open to the idea. However, the only way to get something done in this area is for concerned citizens to try it. There are now at least three companies either making or planning to make computerized voting booths and, according to the FEC, they all intend to rely on secrecy of operation for security. Oddly, none of the companies have named their flagship products "The Titanic".

Do you think these people have developed perfect, unbreakable codes? Some associates of mine and I think not. In fact, we have begun to formulate some testing strategies. I've done a lot of work myself, but I now need some expertise in the areas of cryptography, decompiling programs, and MS-DOS on IBM PC.

Perhaps we can avoid having a Marcos-Aquino style problem here in America.

Kurt

Our Economy Is Based On Electricity

Jared M. Spool <Spool@SCRC-STONY-BROOK.ARPA>
Tue, 25 Feb 86 11:47 EST

Last week, on payday, I was informed from our efficient payroll department that my bank account would not be credited with my automatic deposit of my paycheck for a couple of days. The reason that was given was a "Power Blackout In The LA area". (Our payroll is handled out of our LA office, while R&D is on the east coast. I don't know the reason for this polarization. I think it has to do with opposites repelling or something.)

A lot of our economy is based on things that use electricity. While battery backups are not uncommon in computer systems, what percentage can withstand a 24 hour blackout? How about 48 hours?

If NY were hit with a 48 hour blackout, what would happen to the NYSE?

I realize that there are lots of social things that happen during blackouts (like rioting and baby booms), but these things tend to be localized to the area of the outage. But, as I stated above, I need a cross country connection to get paid. How much of our economy would be downed because of something like this?

Misdirected modems

Jared M. Spool <Spool@SCRC-STONY-BROOK.ARPA>
Tue, 25 Feb 86 11:31 EST

> From: Alan Silverstein <hp-sdd!hpfcla!ajs@nosc.ARPA>
> Date: Mon, 24 Feb 86 11:12:54 pst
> Subject: misdirected modems
>
> Twice recently, computers at our company (Hewlett-Packard) have been the embarrassing causes of telephonic annoyance. Phone numbers entered incorrectly in uucp L.sys files, due to typos or misunderstandings, have led to systems repeatedly calling private telephones in Fort Collins.
>
> [...]
>
> I bet this happens a lot more than anyone realizes or admits.

I'll admit it. Four jobs ago, I worked at (what was then a startup) as one of two developers on a electronic mail package using regular phone lines as the network. We used to test the product, over night, by having the five test machines try to send and receive 100-200 messages (per machine) over the five phone lines. (We did this in batches of 20 messages.) The tests were set to start anywhere from 11:00 p.m. to 3:00 a.m. and could go 2-3 hours in length depending on how we set them up. Different machines would have different starting and length times.

The product worked, such that if the phone was busy or didn't answer, (the modem couldn't detect the difference,) it would try again after a certain delay (approx 15-20 minutes) until it failed 10 times. The test was set up that each batch would generate only one phone call.

One morning, after running such a test, I noticed that, on one of the machines, all of the batches set to go to a second machine didn't make it, while all of the batches for the other three machines did. On further investigation, I determined that the phone number for the second machine was incorrectly typed into the sending machines database. It turned out to be a residence, and an apology was made. We double checked our test sets before starting them, after that.

In conclusion, it is very easy, with today's technology to do such a thing. Modem technology has even progressed that the modems themselves redial the numbers until a connection is made, with no regard to the fact that there will never be a machine on the other end.

We have always had wrong numbers. However, when a human dials a wrong number, there is (almost) immediate confirmation that the number is wrong, and a second or third or tenth retry is not attempted to the same number.

Maybe what we need is a touch tone code (or something) that one can enter into a modem that says "The number you have is wrong, go away."

The Titanic Effect

<Boebert@HI-MULTICS.ARPA>
Tue, 25 Feb 86 18:21 CST

This rule is, I believe, actually an instance of the 28th Axiom of Systematics: "When A Fail-Safe System Fails, It Fails by Failing to Fail Safe." All 32 Axioms, the Four Basic Postulates, and Corollaries can be found in the delightful _Systemantics_ by John Gall (Quadrangle/NYT Books, 1977, ISBN 0-8129-0674-8), which deserves to be better known.

Earl

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 2: Issue 17

Friday, 28 Feb 1986

Contents

Replacing humans with computers?

Nancy Leveson <nancy@ICSD.UCI.EDU>
25 Feb 86 22:06:36 PST (Tue)

I have recently seen several risks contributions which assumed that humans are the cause of most system accidents and that if the human was somehow replaced by a computer and not allowed to override the computer (i.e. to mess things up), everything would be fine. The issue is too complicated to cover adequately here. But before rushing off to replace human controllers with computers, at the least consider the following:

** Most accidents involve multiple failures of different components
   of the system. It is rarely possible to pinpoint one particular
   failure as the sole cause. (e.g. Three Mile Island involved at
   least four or five different types of mechanical failures. Who
   got the blame?)
** There are often powerful and compelling reasons for wanting the

blame placed on the human. For example, Babcock and Wilcox can
be sued for billions if there is something wrong with the design
of their nuclear power plants -- how much can you collect from
some poor operator?

** The human is often called in to save the day after chaos has
already begun and then expected to come up with a miracle. If he
does not save the day, then the blame is often placed on him/her
instead of the initiating mechanical failures.

** Most accidents result from unanticipated events and conditions.
Thus it is doubtful that computers will be able to cope with emergencies
as well as humans do. Expert systems do not help in coping with
unanticipated events or conditions.

** There are many examples of accidents which were averted by a human
overruling an errant computer. If the operator had not intervened at
the Crystal River Nuclear Power Plant, for example, a catastrophe might
have occurred because of the computer error. The hype about "expert
systems" and "artificial intelligence" may be very dangerous.
There are reports that commercial pilots are becoming so complacent
about automatic flight control systems that they are averse to
intervene when failures do occur and are not reacting fast enough
(because of the assumption that the computer must be right).

The problem is just not that simple that the answer "replace the human
with a computer" will solve it.   Nancy

Eastern Airlines stock

Steve Strassmann <straz@MEDIA-LAB.MIT.EDU>
Thu, 27 Feb 86 02:38:17 EST

As an owner of Eastern Airlines stock (fell from $11 to $5 right after I bought it), I'm particularly upset by this. I don't know the details; I hope someone with more knowledge can fill them in.

According to my stock broker (Disclaimer: I don't have any hard documentation, and I'm not a Wall. St. expert), one of the major blows to the already troubled company was a bogus earnings report issued on a Dow Jones computer (something like 20 cents instead of $1.50). The mistake was corrected within the hour, but in that hour, portfolio managers had dumped Eastern stock, and the price fell $3, and never recovered. I think this happened around early September.

Computerized stock trading and feedback systems

<kremen@aero>
26 Feb 86 07:57:40 PST (Wed)

There seems to be some misunderstanding about computerized stock trading.

First, "programmed buys" and "programmed sells" really have nothing to do with computers. All "programmed" transactions could be done by hand but typically they are extremely complex, so a computer is needed. Programmed trading only occurs when special intermarket conditions are present. Program trading consists of arbitrageurs who use the spread between the value of stocks on the New York Stock Exchange (NYSE) and the Chicago Board of Options Exchange (CBOE) in Chicago. Occasionally other markets are used.

Intermarket arbitrage adds to market volatility but not in a negative sense. The infamous "Triple Witching Hour", a time four times a year of extremely volatile trading, is a direct result of this intermarket arbitrage.

Eric Nickell in his note compare the market to a feedback system that oscillates - something like a forcing function with resonance. Well not at all true. The market cannot get really swamped because something will "break-down first". In the case of the NYSE - the "market makers" will have an "order imbalance" preventing further trading.

Computer Voting Booths

Larry Polnicky <Polnicky@HIS-PHOENIX-MULTICS.ARPA>
Wed, 26 Feb 86 10:43 MST

In RISKS Vol 2, Issue 16, Kurt Hyde write:

> There are many documented cases of accidental miscalculation in computerized
> vote tallying equipment. The reasons why such errors were discovered is
> because reconstruction and recount was possible. Investigators
> reconstructed by gathering the machine-readable ballots. They were then
> able to recount by machine or by hand. Such reconstruction is impossible
> with the current state of the art in computerized voting booths because no
> physical ballots are created. Recounts in such cases are wholly dependent
> upon the software to have stored each vote in its proper storage location at
> the time of voting.

While the risks would not be entirely removed, and regardless if any fraud or error is suspected, there could be a standard practice initiated whereby a sample from each election is validated by follow-up phone call or physical notification. Privacy could be somewhat maintained by automating this process, e.g., immediately after the polls close, the computer randomly selects some small sample and sends a letter saying, "Citizens Jones, according to our computer voting system, you voted thusly:...." The citizen then returns the card validating or invalidating his voting record. A box could be checked for him to indicate that he would rather not acknowledge via mail or not at all; the percentage of such respondents would probably be low. Also, since some people may goof or maliciously be inconsistent, the final validation would not have to be unanimous; some standard percentage of validation would pass as I believe it does today in a recount. If delegating the follow-up procedure to a computer is the start of a new computer risk, then it could be done manually, but I believe this kind of check-back mechanism would significantly reduce the risks involved in computer voting to the point that it could gain approval.

Larry Polnicky, Honeywell Information Systems, McLean, Virginia.

Reliance on security

<Jong@HIS-BILLERICA-MULTICS.ARPA>
Wed, 26 Feb 86 12:19 EST

Kurt Hyde's reference to the Phillipine elections and the security of computerized vote-counting systems reminds me that the issue of computer security is artificially narrow. If I am a criminal, and you confront me with an unbreakable computer security system, I will simply direct my attention elsewhere. Attacking strong points went out with World War I (or, to maintain the underworld analogy, with Machine Gun Kelly).

The most elaborately password-protected system is easily cracked if the passwords are transmitted over telephone lines, or if people leave their passwords lying about on scraps of paper. That may fall outside the venue of computer science, but not outside the venue of reality. In the case of the Phillipine elections, it didn't matter how well the vote-counting computers were programmed; there were soldiers at the polling places threatening to shoot voters. Ballot boxes were opened to reveal twenty thousand ballots marked in the same handwriting for Mr. Marcos. The computer operators were being told what numbers to enter.

I guess there's not much you can do about risks outside your direct control. My point is not to get too focussed in our concerns.

[As noted many times in RISKS, any single weak link may represent a vulnerability. In systems designed not to have single weak links, there are weak combinations. Thus we must be concerned with ALL of the weak links. PGN]

AI risks

<Nicholas.Spies@GANDALF.CS.CMU.EDU>
26 Feb 1986 23:19-EST

Today I attended an IEEE videoconference on "Applications of Artificial Intelligence" with Drs. Tom Mitchell (CMU/Rutgers), Alex Pentland (SRI), Peter Szolovits (MIT) and Harry Tennant (Texas Instruments). Aside from some overdriven graphics such that it interfered with the audio, it was an excellent intro to AI (for those concerned with the medium AND and the message).

I asked the question, asked here and elsewhere by others, about the potential legal responsibility of authors of AI software, the most obvious example being medical diagnosis. The answer from the panel was that most AI work now has been done under very controlled conditions, responsibility has never been tested in a court case, and that (possibly) the law applying to publishers of reference books might apply also to AI systems (that is, willful deceit would be punishable but typos and other innocent mistakes would not make a publisher accountable). But according to one of the panel members some AI researchers ARE in fact taking out insurance against possible suits but (paraphrase) "the insurance companies look upon this problem as something of a lark and the insurance emiums are low now" although the same panel member said that (paraphrase) "this may become a very important problem in the future".

I originally phrased the question to ask whether the implicit threat of possible suits against artificial intelligence applications might have a chilling effect on research and development of interesting applications (that is, those involving human life and property), but as it was not asked it was not answered.

My own (legally uninformed) feeling is that AI by its very nature spreads around the concept of "volition" such that the present legal system might have a difficult task in assigning responsibility in a damage suit (and these doubtless will come down the pike someday).

Data Encryption Standard

Dave Platt <Dave-Platt%LADC@CISL-SERVICE-MULTICS.ARPA>
Thu, 27 Feb 86 17:31 PST

There's an interesting article in the 2/24 issue of InformationWEEK concerning the DES. Apparently, DES was up for voting to become an international encryption standard sanctified by ISO. The NSA (National Security Agency) was lobbying very strongly within ANSI (the United States' representative within ISO) to have DES disapproved... the apparent reason being that wide standardization of DES, and its routine use, would make it substantially more difficult for NSA to monitor overseas voice and data communications. IBM pushed very strongly within ANSI for a "yes" vote within ISO (DES is already an ANSI standard, and its details have been readily available to anyone for the past five years or more). In the end, IBM won and NSA lost; ANSI abstained from voting, which had the same net effect as a "yes" vote.

Have any studies been done concerning the risks of having, or not having a secure data-encryption scheme to guard the integrity of one's data?

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 2: Issue 18

Friday, 28 Feb 1986

Contents

Titanic and What did I overlook?

<Murray.pa@Xerox.COM>
Wed, 26 Feb 86 00:24:08 PST

There is also the reverse of the Titanic problem. Sometimes trying to protect against a particular mode of failure that you are very worried about actually makes the overall reliability worse. I'm thinking of the cases where the whole system gets so much more complicated because "fixing" something pushes it over the edge of well understood technology.

The aspect of calculating failure probabilities that has always bothered me is that I can't see any way to take into account the things I have totally overlooked, the areas that I haven't even dreamed about. You know, the sort of problem where, after you hear the story, you sigh, and feel sorry of the people involved rather than thinking that they would have noticed the problem if they had been a bit more diligent when testing. Is there any theory in this area?

I've helped track down several very obscure bugs in hardware and/or microcode. Each time we finally located a problem, I've been amazed at how easy it was to make it happen. That is after we knew where to poke and had set up the right test programs. Two examples come to mind.

Ten years ago, I worked on a PDP-10. At one point, the machine was acting a bit funny. It would run Tenex for days. However, our only big hairy LISP program sometimes got the wrong answer and the bootstrap loader sometimes zeroed itself while it cleared memory. One day, the boot loader trouble got reasonably solid. We wrote a small program to mimic what the it was doing, catch the trap, reconstruct the test sequence, and try again. It didn't fail. We included the previous 6 instructions from the loader into our test sequence. They were doing something totally uninteresting. It failed solidly - every few milliseconds for an hour while we poked around with a scope. We finally found a textbook example of a runt pulse. It was happening just when the end test should decide to stop. (The real problem was a sick power supply.)

Several years ago, I was doing a lot of Ethernet tire-kicking. The early Dandelions were coming out of the factory. Everybody was looking for trouble rather then introducing new problems into their code. Things felt pretty solid. One evening, I was testing some transceivers. Nothing interesting was happening, so I connected in another spool of coax. Poof. Lots of packets started falling through the cracks. Simple tests worked 100%, but more complicated tests would miss 50% of the packets. It was a simple timing problem. If a packet started arriving while the microcode was preloading the transmit FIFO, the microcode/hardware discarded the input packet as it disabled the transmitter while switching modes to go inspect the input packet. By inserting the extra coax, I had increased the delays enough to drop a packet right into the window.

PS: I second Earl Boebert's recommendation for John Gall's Systemantics. If only I could remember all his lessons that seem so simple and obvious while reading about them....

[Maybe you could be COAXed. PGN]

Titanic Effect

<Jong@HIS-BILLERICA-MULTICS.ARPA>
Wed, 26 Feb 86 12:24 EST

I suppose if I had said to the designer of the Titanic: "Yes, the worse maritime accident on record involved the breaching of four watertight compartments, SO LET'S PLAN ON SURVIVING FIVE," the designer would have specified smaller compartments, so that the Titanic would have had eighteen, not sixteen, compartments. And the iceberg would have ruptured six compartments...

Computers placing telephone calls

"Art Evans" <Evans@TL-20B.ARPA>
Wed 26 Feb 86 14:18:23-EST

Some years ago the ARPANet Network Control Center (NCC) at BBN was tasked to check periodically that each dialup line to each TIPs was in fact functional. Absent such a check, a TIP port could be non-operational for a long time before anyone would notice.

To make the check, a computer at NCC was connected to an outward WATS line and programmed to call every TIP line around the country periodically, every week or so, to be sure it could properly connect to a modem. For a busy signal or other failure to handshake with a modem, the program would retry a few times and then alert a human being about a possible problem. Then a person at the TIP site would be asked to check the line there.

All this was OK, and it worked just fine. Once, however, by some accident, the computer was connected to an ordinary phone line rather than to the outward WATS line. The first indication BBN had about this disaster occured when the phone bill came, in a cardboard box, with some three inches thickness of call itemization slips for all those calls. I don't remember the total, but I do remember that it attracted a *lot* of attention at very high management levels. There was much discussion about whether the improper phone connection was BBN's error or the phone company's; I think a compromise was eventually worked out.

A nice check was immediately added to the whole system. The outward WATS line had the property that it could be used to call anywhere in the 48 contiguous states except Massachusetts (which is where BBN is). Thereafter, each night the program placed the first call to a Massachusetts modem. If that call worked, the run immediately aborted and a human was notified that some line other than the proper WATS line was in use.

A lot of problems are easy to solve, once you know what the problem is.

Art Evans

Misdirected modems

<delftcc!sam@nyu.arpa>
Fri, 28 Feb 86 08:09:37 est

Modems and calling software should treat as special the case that the phone on the receiving end goes off hook, but no carrier is detected. This means either that (1) a person has picked up the phone, or (2)

there is some incompatibility between the calling and answering modems,
or (3) there is a bad connection. (3) should also be detectable to a
modem (is this true?), so we eliminate it from the special case. In the
special case the calling software should retry the number a very few
times, then call for human intervention.

Unfortunately, the ultra-standard Hayes Smartmodem 1200 cannot
distinguish between various NO CARRIER conditions at all, much less
distinguish (3) from (1) and (2). Better (smarter) modems are needed
before the calling software can deal with this special case, and stop
its modems from accidentally torturing people.

Sam Kendall allegra \
Delft Consulting Corp. seismo!cmcl2 ! delftcc!sam
+1 212 243-8700 ihnp4 /
ARPA: delftcc!sam@nyu.ARPA

Modems and phone numbers

David Barto <celerity!shipit!barto@sdcsvax.ucsd.edu>
27 Feb 86 13:27:46 PST (Thu)

While setting up a link to a new system, I entered the phone number
incorrectly. I failed to connect when the machine attempted to do the
call. Being very suspect of myself (on the first call), I dialed the
number the machine was attempting to call. A person answered, and I
attempted to determine the phone number she was at. This number was
not the same number I was dialing. I then called the operator (good
old AT&T), and asked what was going on. The operator dialed the same
number, got the same person on the line, and verified the number was
different.

We worked on the crossed lines problem for 2 days.

The final solution was not crossed lines, but the fact that multiple
numbers connected to ONE phone.

Sadly, neither the operator, nor the person answering the phone, had
any idea that multiple phone numbers went to the same physical unit.

How many phones sit on your desk. How many phone numbers will it
ring to. Are you really sure?
--
David Barto, Celerity Computing, San Diego Ca, (619) 271-9940
decvax-\ bang-\ ARPA: celerity!barto@sdcsvax.ARPA
ucbvax-->-sdcsvax->!celerity!barto
ihnp4--/ akgua-/

"Moderation in all things, including moderation"

[Including net addresses? PGN]

Misdirecting my modem

Mike McLaughlin <mikemcl@nrl-csr>
Wed, 26 Feb 86 20:36:07 est

Once upon a time, early in the days of my computer-life, I worked late. I told my Z-120 to tell my Hayes to call a number. It did, and I heard the ring, and then the answer. No whistle-hiss-CONNECT, but a quavery young female voice saying, "Hello?... " I sent three pluses and an ATH to the Hayes, read the (wrong) number off the screen, and dialed it on my voice phone. I wanted to render immediate and abject apologies. The phone rang and rang. I redialed, in case I had incorrectly dialed the wrong wrong number. It rang and rang. I quit. There was no way to un-scare that young woman. I have been much more careful since then - but still ring a wrong number now and then. If it is during the day I voice-phone to apologize. If it is in the wee hours, I just say a prayer for that person's serenity, and mine, and go on.

It seems common courtesy to check all supposed "computer phones" by voice, by day, prior to using them in an auto-dial mode. The computer doesn't lie awake at night wondering what wierdo is ringing the phone and hanging up.

- Mike McLaughlin

Power-outages, & other failures of central DP systems

Dave Platt <Dave-Platt%LADC@CISL-SERVICE-MULTICS.ARPA>
Wed, 26 Feb 86 12:11 PST

In my experience, battery backup for computer systems is usually of extremely limited capacity (an hour or two) when you're talking about a large computer center with lots of power-hungry disks and so forth. Frequently, the amount of battery storage capacity is enough to permit the system operators to shut down their machines in a graceful fashion, and requeue any work-in-progress for processing when the AC mains come back up. Sites that absolutely require uninterruptable power generally have backup diesel generators... they're much smaller per kilowatt than batteries would be, and can run for days at a time as long as you keep feeding them fuel.

I'm not sure what would happen to the NYSE if there were a two-day blackout in New York. There was an extensive blackout (six hours or so???) back in the 60's, I seem to recall... but it was shorter than the one that you're speaking of, and the NYSE is probably much more dependent on computers than it was twenty years ago. I imagine that they'd probably have to shut down.

I read a book recently that might be of some interest to Risks readers, as it addresses the problems of centralized data transmission and storage to some extent. The book is "Night of Power", by Spider Robinson; it's

fictional, borderline SF [by my standards... open to dissent], and
revolves around the seizure of Manhattan Island (and the East Coast's
major satellite uplink) during a social revolution in the 1990's. The
point was made that the seizure of the uplink could easily have resulted
in a major collapse of the world's interlinked financial systems, if
the data flowing through the link were to be cut off or corrupted.

Computer voting booths

Dave Platt <Dave-Platt%LADC@CISL-SERVICE-MULTICS.ARPA>
Fri, 28 Feb 86 12:10 PST

GAAK! Maybe I'm misunderstanding [Larry Polnicky], or the systems actually used in the computerized voting booths... but I had always believed that the voting systems in this country [paper, computer-based, or whatever] were designed to GUARANTEE A SECRET BALLOT! I've NEVER heard of a public-voting system that was designed to permit anyone to identify a particular vote, or set of votes, with a particular voter. There is a longstanding tradition in this country of guaranteeing that an individual can vote his or her conscience, without being identified afterwards as "the person who voted for Smidget for Congress".

There have been plenty of examples in the past of the problems that can occur when a person's votes are not kept secret. Both in this country, and in numerous countries overseas, people who have voted the "wrong way" (usually against a clique in power) have been pressured, fired from their jobs, beaten, tortured, or killed. I would strongly resist any computerized (or paper) voting system that would make any votor's voting record identifiable to *anyone* without that votor's explicit approval.

Note here that I'm not talking about voting systems such as Congress uses, in which the public has an explicit right to know who voted for & against what. In systems such as this, it's fine to have records kept, and some sort of accuracy/accountability audit... but by their very nature, these systems are generally much smaller than state-wide or national voting systems, and are thus less likely to be subject to large-scale fraud.

[Even in paper ballot systems, there is usually a serial number which provides a back-link from the voter to the ballot. Otherwise fraud is far too easy, with mystery ballots appearing out of nowhere. But recall the earlier Phillipine election in which a local power failure downed the central ballot-counting computer, which upon reboot immediately finished the ballot counting. Somebody has to be trusted somewhere. There is a choice as to whom the trust must be given. PGN]

Re: Data Encryption Standard

Chris McDonald <cmcdonal@wsmr06.arpa>

Fri, 28 Feb 86 12:47:35 MST

In response to the DES item, the National Security Agency and other US
intelligence services have conducted numerous signal intercept exercises
throughout the US. The results of such exercises are for good reasons
classified under national security directives. Readers Digest, however, which
obviously has good connections, has published several articles during the last
5 years describing the threat from foreign intelligence services as well as
from industrial espionage. IEEE Spectrum publication had an excellent article,
"Thwarting the Information Thieves," in its Jul 85 edition.

Presently under Fed Standard 1027 DES devices are export controlled items.
This would means that US firms who build such encryption hardware must obtain
an export license before any foreign sale. Since NSA is the author of the
Standard, their position would seem to be consistent. IBM of course does sell
and build DES devices, and its personnel developed the algorithm upon which DES
is based. Therefore, their position would seem to be consistent.

Chris McDonald
White Sands Missile Range

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 2: Issue 19

Sunday, 2 Mar 1986

Contents

A word from Isaac Asimov about Robots.

<crash!bryan@nosc.ARPA>
Sat, 1 Mar 86 13:45:11 PST

I went on vacation last week, irrelevant I know except for the following.

I flew on American Airlines, which had for the amusement of its passengers an in flight magazine called "American Way" issue dated February 18, 1986. It contained an article written by Isaac Asimov which I have reproduced here. The clever pictures by Kent Robbins also in the article were omitted for obvious technical reasons.

Robots! Beware!
by
Isaac Asimov

reprinted from American Way, February 18, 1986.

I invented the Three Laws of Robotics in 1942, and these laws, which are built into the robots of my science-fiction stories, prevent them from harming human beings, force them to follow orders,a nd make them protect themselves, in that order of importance.

Of course, the robots in which I imagined these laws to exist are complex fictional robots, far more advanced than anything in real life (as yet). In contrast, the robots in industrial assembly lines right now are just computerized arms, capable of doing simple tasks over and over.

But they are capable of doing harm, and, as the inventor of the laws, I always feel guilty.

Two workman in Japan were killed by robots, and in July, 1984, there was the first fatality in the United States. When the first American was killed by robots, there were 13,000 robots in in industrial use in the United States. One such accident with 13,000 robots in existence doesn't seem like a bad ratio, but it is estimated that by 1990 the number of industrial robots will reach 100,000. Will the rate of robot-caused fatalities also increase eight-fold?

One may argue that accidents occur in connection with almost every mechanical device, however simple and small. Yet robots are different. Because they seem more intelligent than other machines, a fatal accident seems more likely to be the result of there malevolence. There is the feeling that intelligent machines should be more careful and avoid hurting a human being. In short, even if I hadn't invented the Three Laws of Robotics, people would take it for granted that they ought to exist.

People therefore would resent robots more than they would resent other devices that do harm; a robot should know better.

If we're living in a society that is going to be more and more robotized, then a public that resents and fears robots is likely to cripple what we think of as progress.

Yet the serious accidents that have taken place so far in connection with robots have been the result. at least in part, of human carelessness.

Perhaps in place of the first law we need a substitute that puts the onus on human beings. The first law --"A robot may not injure a human being, or through inaction, allow a human being to come to harm"-- cannot be built into the simple robots of today, so maybe it should be replaced with "A human being must not approach a robot in operation or one that may suddenly become operable."

In other words, the human being must stay away. In order to reinforce that, the robot must be surrounded by a barrier, ideally one with a gate that when opened to allow human beings access will cut off all power to the robot.

Unfortunately, a barrier is sometimes insufficient. If it can be climbed or crawled under, there is nothing to prevent someone from doing that rather than taking the trouble to open the gate. (Why? It's hard to explain, but we see human beings risking their lives every day in order to save 15 seconds of time.)

As a result the barrier must not simply consist of railings or a low fence. It should consist of an elaborate fence that only can be penetrated by way of a gate.

Furthermore, people who work with robots (of the kind we have now) must be thoroughly indoctrinated with the understanding that a robot that is not in operation may have inactivity as part of its cycle and that if the power is not off, the robot may suddenly move into operation as another part of its cycle begins.

There might be emergencies when human beings must approach robots in operation. If so, it is unsafe to suppose that they can count on a robot continuing a motion indefinitely no matter how often it repeats the motion. It is possible that the robot's programming calls for repeated motions of a particular sort, but eventually, a set of different motions will start as another part of the cycle begins.

To help understand this, there should be clear markings on the floor and other work areas representing the extreme range of all robot movements in all directions.

Since no matter what one does, experienced workers begin to be overconfident of their own abilities and contemptuous of the robot's ability to do harm, indoctrination should be repeated periodically, and any violation of safety rules invariably should be followed with disciplinary action.

Eventually, of course, when robots have grown sufficiently complex, the three laws may be built into them, and then take over the responsibility for human safety, and we can relax.

====================

Isaac Asimov report's that the word "robot" is of Slavic origin and was first used in a play, "R. U. R." written by a Czech playwright, Karl Capek, in 1921. The initials stand for Rossum's Universal Robots. In Czech the word refers to "involuntary servitude."

Re: AI risks

<epiwrl!shore@seismo.CSS.GOV>
Sat, 1 Mar 86 07:32:52 EST

Expert systems are inherently untrustworthy.

If you claim or imply otherwise,
and if the system subsequently causes harm,
and if those harmed sue you,
you get what you deserve.

John Shore

Re: Replacing Humans with Computers

David desJardins <desj@brahms.berkeley.edu>
Fri, 28 Feb 86 20:47:58 pst

Nancy Leveson <nancy@ICSD.UCI.EDU> writes:
>I have recently seen several risks contributions which assumed that humans
>are the cause of most system accidents and that if the human was somehow
>replaced by a computer and not allowed to override the computer (i.e. to
>mess things up), everything would be fine.

I really don't think anyone is proposing this. What people are proposing is the use of computers to monitor data and alert humans to potentially dangerous situations. My understanding is that even minor failures at nuclear power plants activate hundreds of alarms and warning indicators. Clearly what is needed is an expert system to analyze the mass of incoming data and summarize the situation to the human staff. It can also react, more quickly than humans can, but presumably it would be designed to seek human approval before taking any drastic action.

On-line Slot Machines

Jeff Makey <Makey@LOGICON.ARPA>
28 Feb 86 15:53 PST

The following article, reproduced here in its entirety, appeared in the 25 February 1986 edition of the San Diego Tribune.

Can Nevada handle new slot gimmick?

LAS VEGAS (AP) - A slot machine promotion promising payoffs of $10 million to $15 million has been given the green light by the Nevada Gaming Commission, but not without some misgivings.

Commission Chairman Paul Bible said he had reservations about slot cheats who might rig the machines for phony payoffs. The progressive slot machine network, known as Megabucks, would be available in numerous hotels throughout Nevada and would be linked by a computer system to build up the huge jackpots.

Ray Pike, an attorney for Megabucks manufacturer International Gaming Technology, said the company has made every effort to make the machine cheat-proof.

It sounds like they are using some sort of computer network to link a bunch of slot machines together. Without knowing more than the above about the system it's hard to tell if they have vulnerabilities that other financial networks (like ATMs) don't have. Cheating a slot machine is not the same (in most people's minds, I suspect) as stealing from a bank, so -- with $10+ million at stake -- I'll bet (pun intended) that someone will try to break the system soon.

◀ ▲ ▶ ℹ ✎

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 2: Issue 20

Sunday, 2 Mar 1986

Contents

Risks in Encryption

<Saltzer@Athena.MIT.EDU>
Fri, 28 Feb 86 19:01:21 est

Dave Platt asks:

"Have any studies been done concerning the risks of having, or not having a secure data-encryption scheme to guard the integrity of one's data?"

Studies I am not aware of, but my own informal observations suggest that one of the biggest risks in using good quality encryption is that when you come to use the data you may discover that

a) you have misplaced the key
b) it was encrypted with a different key than you thought
c) a few bits have been damaged in storage
d) something else went wrong

and the data is unusable garbage. All these problems can be avoided, of course, but only if very careful system design is applied to key management and verification that the encryption was done right. The

way to think of the problem is as follows: before you delete the
original cleartext you would like a very credible proof of the
theorem that "this stuff will be decipherable six months from now
when I want it." After thinking about it you may decide to simply
copy the cleartext to a floppy disk and lock it in your desk. At
least then you have some intuition about the list of threats you are
up against.

Jerry

NSA and encryption algorithms

<ulysses!burl!rcj@ucbvax.berkeley.edu>
Sat, 1 Mar 86 14:56:43 est

>international encryption standard sanctified by ISO. The NSA (National
>Security Agency) was lobbying very strongly within ANSI (the United States'
>representative within ISO) to have DES disapproved... the apparent reason
>being that wide standardization of DES, and its routine use, would make it
>substantially more difficult for NSA to monitor overseas voice and data
>communications. IBM pushed very strongly within ANSI for a "yes" vote

This is not the first time NSA has tried to stomp an encryption standard
for these reasons. A few years back several business organizations (mostly
major banks and other financials) got together and came up with an
algorithm involving encrytion keys that were HUGE prime numbers (like
50-100 digits) to use in protecting sensitive financial data transmissions.
NSA stepped in and put tremendous pressure on them not to use this algorithm
-- seems it would take all their Crays about 3-4 days to break any given
transmission. The pressure worked, the idea was dropped.

The MAD Programmer -- 919-228-3313 (Cornet 291)
alias: Curtis Jackson ...![ihnp4 ulysses cbosgd mgnetp]!burl!rcj
...![ihnp4 cbosgd akgua masscomp]!clyde!rcj

P.S.: I really don't remember where or when I read this, so correct me
(publicly, if I am wrong enough) if you can and don't ask me for more details
'cause that's all I remember. Thanks!

Low-Tech Computerized Voting

"Harry S. Delugach" <hsd%virginia.csnet@CSNET-RELAY.ARPA>
Fri, 28 Feb 86 10:29:10 est

Our local elections are tabulated by computer. The balloting itself uses
that ancient (but tangible) 80-column punch card placed in a holder with
candidates' names, The voter uses a little punch next to the name. After
voting, the card is placed in a sealed counter, under the eyes of a polling
official. Each ballot comprises a single card -- if you make a mistake, the
election official tears up the card and gives you a new one. This method is
a long way from the technologist's state-of-the-art, but it fosters public

confidence in the vote count, because each ballot exists as a piece of paper.

My father has been a polling judge for many years. His precinct (in another state) uses mechanical voting machines. To ensure an accurate count, one person reads the total off the machine while a second person watches to double-check. A third person writes them in ink on a paper tally sheet, while a fourth person double-checks. After the tallies are made, the *entire machine* is sealed and sent downtown for checking. It would involve the complicity of lots of pairs of people in many locations to make ballot-stuffing work, and not just (perhaps) one or two dishonest programmers. Not high-tech, but still reliable.

As the Philippine election suggests, the public's highest priority is its trust in poll workers and the honesty of the count. The speed of the count is not as important.

Risks in ballot-counting systems

<hplabs!topaz!harvard!wjh12!maynard!campbell@ucbvax.berkeley.edu>
Sun, 2 Mar 86 23:10:08 est

> [Even in paper ballot systems, there is usually a serial number which
> provides a back-link from the voter to the ballot. Otherwise fraud is
> far too easy, with mystery ballots appearing out of nowhere. But
> recall the earlier Phillipine election in which a local power failure
> downed the central ballot-counting computer, which upon reboot
> immediately finished the ballot counting. Somebody has to be trusted
> somewhere. There is a choice as to whom the trust must be given. PGN]

I've never seen a voting machine, so I can't comment on them. But I have been active in Massachusetts state and local politics for a few years and have always voted on paper ballots. I've *never* seen any sort of serial number and would be shocked to see such a thing.

When I vote, the following steps are involved:

1. I go to the first table and tell the person there my name and address. She crosses my name off the voting list.

2. The person at the next table hands me a ballot. There is no serial number on the ballot, and no notation is made on the voting list other than to cross off my name.

3. I mark my ballot and go to the other side of the room (away from the voting list table).

4. A person there, at the ballot box, takes my (folded) ballot and inserts it into the ballot box slot. While I watch, the crank is turned to suck the ballot into the (locked) box.

There are a number of techniques used to prevent fraud.

1. Each political party designates one or more observers to oversee both the polling place and the counting of ballots. Of course the observers are biased, but in opposite directions that hopefully cancel out.

2. The ballot boxes used here have a slot into which the ballot is inserted and a crank that's turned to suck it in. I don't know, but the crank could also stamp the precinct number on the ballot. If fraud is suspected, you'd look for precincts turning in more ballots than they had registered voters.

3. The voting procedure is open to challenge at any time. Voter lists are public information and are scrutinized before the election by political workers (I know, I have done this for a campaign). Anyone can go up to the polling place and challenge a vote ("I think Joe Shmoe is a pseudonym and I challenge his ballot"). When Joe Shmoe votes, his ballot is set aside as a challenged ballot and is verified separately. Of course, in this case his ballot is marked (I presume by being placed in a sealed envelope with his name on it) but if he is verified as a legitimate voter then his ballot can be mixed in with the other ballots anonymously. (Just like an absentee ballot.)

Of course, once the ballot is cast it's anonymous and can't be challenged in particular. When I worked as an observer at the polls we were encouraged to challenge any voter or name that looked the least little bit fishy (of course, the unspoken rule was you'd only challenge voters wearing a button for the opposition). It doesn't hurt to challenge a ballot that turns out later to be valid (other than annoying the precinct workers) but if you fail to challenge a truly invalid ballot, it's pretty difficult to do anything about it after the fact.

Sorry about the length, but the gist of this is that, around here anyway, once you investigate you find that there are enough checks and balances to make fraud (not impossible but) unlikely, and also to guarantee secrecy.

If voting operates substantially differently in other parts of the country I'd be interested in hearing about it.

```
--
Larry Campbell                             The Boston Software Works, Inc.
ARPA: maynard.UUCP:campbell@harvard.ARPA       120 Fulton Street
UUCP: {harvard,cbosgd}!wjh12!maynard!campbell  Boston MA 02109
```

Misdirected modems

Richard H. Lathrop <RICKL@OZ.AI.MIT.EDU>
Sun, 2 Mar 86 07:58 EST

RISKS-LIST: RISKS-FORUM Digest, Monday, 24 Feb 1986 Volume 2 : Issue 14

From: <hp-sdd!hpfcla!ajs@nosc.ARPA>

> Date: Mon, 24 Feb 86 11:12:54 pst
>
> Twice recently, computers at our company (Hewlett-Packard) have been the embarrassing causes of telephonic annoyance. Phone numbers entered incorrectly in uucp L.sys files, due to typos or misunderstandings, have led to systems repeatedly calling private telephones in Fort Collins. The recipients of such calls, understandably annoyed, have had to backtrack through Mountain Bell to discover the cause.
>
> I bet this happens a lot more than anyone realizes or admits.

Yes, I suspect this does. I am reminded of a time several years ago when I was in Oregon working on a tide-monitoring system for NOAA (Natl. Oceanic & Atmospheric Admin.). They were interested in accurate measurements of tidal depth for navigation charts, storm surge & tsunami monitoring, etc., and we developed a remote station for them which would measure the water depth to the nearest 1/100 inch every 6 minutes and store the data in internal memory. There were several of these scattered along the coasts and Great Lakes, and every couple of days a master controller would call them all up (at midnight, to take advantage of lower phone rates & line activities) & drain their data.

At the time I was writing the Assembler telecommunication subsystem and a partner was writing the Fortran user-interface and control system. Since we only had one development machine, I was on a night schedule & he was on days. Predictably (by 20-20 hindsight), while testing one midnight the call was answered, not by our remote, but by a very sleepy & puzzled Michigan housewife (2:00 am there). I suddenly found myself on the line trying to explain that I was not a prankster, but that my computer had dialed her up from Oregon and warbled at her, by mistake.

Of course, a typo had been made in the data file that specified the phone numbers. One thing to note about this incident is the separation between the specification function (done on the daytime schedule) and the test function (nights). While it is always possible to err, this separation precluded the possibility that we could cross-check each other.

-=*=- Rick Lathrop

rickl%oz@mit-ai

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 2: Issue 21

Monday, 3 Mar 1986

Contents

The risks of (not) using Robots

<Murray.pa@Xerox.COM>
Mon, 3 Mar 86 18:56:03 PST

Workers are very good at bypassing systems designed to protect them. Ducking under the fence to jump in front of the robot is just the tip of the iceberg. Ask anyone who has worked around big machinery.

The standard interlock for a hand fed press is a pair of big buttons, located at waist level, one on each side. You have to press both to start the cycle. The operator is expected to use one hand on each button, and hence can't have any fingers in the danger zone. Tape, feet, hips, boards, ... The list is endless. (That description may be out of date. OHSA has issued reams of rules over the past 10 years.)

If you have never seen the sort of press I'm thinking of, imagine a machine that's 8-10 feet square at the base, 15 ft tall, and very sturdy. It's got a lot of steel. There isn't any plastic in sight. There is a motor that pumps up a big flywheel. Push the button(s), and a clutch engages and the a crankshaft to turn the rotary motion of the flywheel into an up-down motion driving a set of dies. Each ker-whump, it spits out a piece of bent metal with holes in the right places. Small ones make beer can openers and that size parts. Bigger ones make fenders and washing machines from flat sheets of steel. This sort of machine is the bread and butter of factorys. A row of them is a very impressive

sight and sound. They don't slow down at all if you leave your fingers
in the way.

The more robots we use, the more people will get injured or killed by robots. The critical thing to notice is that most robots are being used in places that were very dangerous for humans, and hence are probably saving lives. (I think painting cars is the prime example.)

Anybody know where to get good numbers?

We need to consider the RISKS of not using robots/computers/you-name-it as well as the RISKS of using them. Sure, we need to look for ways to make things safer, but we shouldn't dismiss an idea because it isn't 100% safe. In fact, if we don't use robots enough, we are costing lives. (Wait 'till that one hits the courts.)

To complicate things, people (and courts) get very irrational when considering emotional issues like robots taking over jobs.

[OK. Remember, someone loses either way. The question is this: which loss is socially least reprehensible? Optimization depends strongly on your viewpoint. A mining company has a view very different from that of the miner, which in turn differs from that of the ecologist. (Don't get caught in a robot of mine without an ore, or you'll have to pretend you are Ingot Berg-man. Sorry. That one smelt bad, but I have been trying for too long to remain unemotional about the risks of a robot taking over the RISKS Forum.) PGN]

Computerized Voting Booths

<Polnicky%PCO@CISL-SERVICE-MULTICS.ARPA>
Mon, 3 Mar 86 07:30 MST

[This is Larry's response to Dave Platt's response in RISKS-2.18
to Larry Polnicky's statement in RISKS-2.17..

> Date: Friday, 28 February 1986 15:10 est
> From: Dave Platt <Dave-Platt at HIS-LA-CP6>
> Subject: Computer voting booths [FULL TEXT IN RISKS-2.18]
> To: Larry Polnicky <Polnicky at HIS-PHOENIX-MULTICS>
>
> GAAK! Maybe I'm misunderstanding you, or the systems actually used in
> the computerized voting booths... but I had always believed that the
> voting systems in this country [paper, computer-based, or whatever] were
> designed to GUARANTEE A SECRET BALLOT! I've NEVER heard of a
> public-voting system that was designed to permit anyone to identify a
> particular vote, or set of votes, with a particular voter. ...

I understand the concerns for privacy. Perhaps the sample that is checked-back could give prior permission. I'm sure there would be some who would give up that right to privacy for the sake of helping to ensure a more reliable election. I would. Indeed, many of us do when we discuss politics around the office and reveal for whom we voted. Last election, I voted by absentee ballot, which associates my name with my vote, though granted not on the ballot itself, but on the envelope in which it is mailed. Computerization has its costs; computer risk reduction will also cost something.

Larry Polnicky, Honeywell Information Systems, McLean, Virginia.

> [Once again, we tend to make naive assumptions that ignore the presence of back-pointers, audit trails, system programmers, maintenance folks, etc. But then, we love to oversimplify. The name of the game is to anticipate all reasonable risks, and then to make sure your design covers many of the unreasonable ones as well -- just in case. Audit trails (for example) can be of great help (albeit after the fact), but they too can be bypassed, spoofed, or misused. PGN]

No-carrier detection by misdirected modems

Dave Platt <Dave-Platt%LADC@CISL-SERVICE-MULTICS.ARPA>
Mon, 03 Mar 86 11:01 PST

Some modems (such as the Racal-Vadic VS212P, of which I own one) do have a voice-detection feature. The VS212P can be optioned to determine that there is something on the line which is neither (a) a carrier, (b) a busy signal, or (c) a ringing signal; it submits the string "Voice!" through the RS232 port, waits ten seconds, and hangs up.

There are two slight problems with this, though... the modem is NOT Hayes-compatible (although I understand that later models are), and the voice-detection feature is not 100% reliable... it's possible for the modem to fail to detect voice, or to report voice detection when it should be reporting busy. For that reason, the modem's standard option setting disables voice detection.

I wonder what the results would be if all autodialing modems (& their software) did consider voice-detection [or anything other than carrier or busy] to be a "trouble" condition that requires human intervention before calling that number again. My experience has been that a substantial number of calls that "should" go through normally don't, for one reason or another... congestion in a private phone network (the network switch recording says "All circuits are busy, please stand by"), failed long-distance trunk, destination system is down and is not answering the phone for the moment, noise on the line that prevents carrier detection / scrambler latch (not uncommon on long-distance calls using the 212 protocol), and so forth.

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 2: Issue 22

Wednesday, 5 Mar 1986

Contents

Voting receipt

Mike McLaughlin <mikemcl@nrl-csr>
Tue, 4 Mar 86 09:47:20 est

Pardon my paranoia, but I would rather not agree, in advance, or afterwards, to have my vote audited for whatever good purpose. Absentee ballots are a problem that I don't worry about too much today... but I might tomorrow.

Besides privacy/secrecy/retribution concerns, I might just forget... or lie... about how I voted. I don't want to be asked to have my vote audited. The fact that I accept or reject the request tells Big Brother something about how I voted.

Therefore, I suggest that the magic voting machine *offer* me a voting "receipt" as soon as I complete my manipulation of its levers or buttons. The "receipt" would contain the date, time, machine number, serial number of the vote, and name the candidates and issues for or against whom/which I voted. It would NOT list my name. The precinct voting records would show only that I voted, in such a fashion as to prohibit tracking of my name to my receipt number.

If I rejected the receipt, it would fall into a locked hopper, openable only
upon completion of the voting period.

If I accepted the receipt, I could check it immediately for accuracy, and ask
for a corrective procedure. If it was OK, I could save it for a possible
recount; or trash it/burn it/shred and eat with milk & prunes, whatever.

Machine-retained receipts could be sampled against the retained electronic
record by voting authorities.

In the event of a recount, I could return my receipt to the voting organization directly, or through a third party/blind drop/cutout or whatever.

My receipt should probably also carry a checksum or other method of making it
difficult to tamper with the receipts.

This proposal is neither fool- nor dictator-proof. It does provide a method
for personal vote checking, a recount method, and preserves personal
anonymity.

- Mike McLaughlin

Re: Voting booths

"Jim McGrath" <MCGRATH%OZ.AI.MIT.EDU@XX.LCS.MIT.EDU>
Tue 4 Mar 86 22:44:16-EST

> From: Dave Platt <Dave-Platt%LADC@CISL-SERVICE-MULTICS.ARPA>
> .... There is a longstanding tradition in this country of
> guaranteeing that an individual can vote his or her conscience,
> without being identified afterwards as "the person who voted for
> Smidget for Congress".

Actually, the "longstanding tradition" is less than a century old (quite
short when you consider our history as spreading back hundreds of years into
colonial times). Until a wave of reform around the turn of the century, it
was quite usual for the state not to provide any ballots at all. Instead,
individual voters or local officials would provide the necessary paper. As
time went on, it became common practive for the political parties to provide
the ballots used in the election. Since ticket splitting was difficult, and
these ballots were quite distinctive, voting was hardly secret (I recall
that in the El Salvador Presidential election a few years ago the ballots
were of a different color, and the box was clear, making voting an open act).

All this information from my reading a few years back of the 3 election
volumes of the California State Code.

Jim

Computerized Voting

Tom Benson <<T3B%PSUVM.BITNET@WISCVM.WISC.EDU<>
Tue, 4 Mar 86 16:27 EST

Larry Polnicky and others have recently been discussing the risks of computerized voting. Surely the first principle ought to be the protection of secret balloting rather than the promotion of the possible convenience of computerized vote-counting. There is a (perhaps slightly cumbersome) solution to the problem of checking accuracy. Suppose an electronic voting booth, with a screen and some sort of simple keyboard. In effect, a menu-driven ballot on the screen. The voter fills in his or her choices and has a chance to go back and correct errors. At that point, the voter pushes a button to confirm the ballot, and a printer prints card ballot, which it retains behind a transparent screen (it can be read but not altered). Voter scans the printed card and is asked whether it is accurate. At this point, if it is not, a REVISE or CANCEL button is pushed and the process starts over with nothing having been recorded (the card is shredded). When the screen and card match the voter's intentions, a second CONFIRM button is pushed and the card is ejected, while the vote is electronically forwarded. The voter takes the card out of the booth and drops it in a ballot box.

This system would permit absolute secrecy for the individual voter, who could not be traced to the card or the electronic vote. But the cards would be in a ballot box, where they could be counted by hand. After the election, a representative random sample of precinct boxes would be counted by hand, and matched to the electronic tally, just to audit accuracy. And in the case of a re-count, the entire election result could be counted by hand.

Tom Benson, Department of Speech Communication,
The Pennsylvania State University, 227 Sparks Building
University Park, PA 16802   phone 814-238-5277

{akgua,allegra,ihnp4,cbosgd}!psuvax1!psuvm.bitnet!t3b   (UUCP)
t3b%psuvm.bitnet@wiscvm.arpa (ARPA)
T3B@PSUVM   (BITNET)

Re: Replacing humans with computers

Alan M. Marcum, Consulting <sun!nescorna!marcum@ucbvax.berkeley.edu>
Mon, 3 Mar 86 19:57:58 PST

In Risks-2.17, Nancy Leveson comments that

> There are reports that commercial pilots are becoming so complacent about automatic flight control systems that they are averse to intervene when failures do occur and are not reacting fast enough (because of the assumption that the computer must be right).

While that may be true, one of the things I learned very early during flight training (I have a private pilot's license with an instrument rating) is to constantly cross-check indications or directives from an autopilot, navigation system, or flight control system. If I have any reason to suspect the autopilot or the navigation instruments (whether it be a fault, or a low vacuum indication for vacuum-driven flight instruments), I take corrective action. It's my life up there, and those of my passengers.

Electricity's power

Marianne Mueller <MASHA@WASHINGTON.ARPA>
Tue 4 Mar 86 20:45:07-PST

Monday saw the complete silencing of the cs lab at the Univ of Washington. "A 13,000-volt feeder cable broke down from 1 a.m. till 4 a.m. but some buildings on the east side of campus were without power till late in the morning." (UW Daily, campus rag.)

Although the U's electric system is separate from the city's, "The blackout in (60 surrounding blocks) occurred when the surge from the University shutdown `jumped' the City Light circuit breakers that would normally prevent the spread of a blackout. Three major City Light circuits were overloaded," the Daily notes.

So no one could do anything on Monday, the terminals were mercifully blank, the halls deserted. The hospital, however, ran on emergency power for three hours, and they got plenty worried about it. Our computers died since 3 hours without air conditioning was more than they could take.

Just for the record.

Marianne

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 2: Issue 23

Thursday, 6 Mar 1986

Contents

Computerized voting

Jeff Mogul <mogul@su-shasta.arpa>
5 Mar 1986 2307-PST (Wednesday)

> From: <T3B%PSUVM.BITNET@WISCVM.WISC.EDU> (Tom Benson)
> Subject: Computerized Voting
>
> After the election, a representative random sample of precinct boxes would be counted by hand, and matched to the electronic tally, just to audit accuracy.

I'm afraid of the seeming reasonableness of this "solution". If we are using the audits to look for fraud in ballot-counting, then "who chooses the `representative random sample'" becomes the interesting question; votes, unlike decaying nuclei, are not uniformly distributed. People who tend to vote for candidate X might live in certain precincts (i.e., black people); might vote at certain times of day (9-to-5 working people); might vote by absentee ballot (older people). If I had the ability to "cook" a voting machine, I might just as easily have the opportunity to cook the "random audit selector".

If we are using the audits to detect failures, rather than fraud, then we must still check every machine and for all times of day, for the same reason: to avoid disenfranchising a segment of the electorate, whether inadvertently or intentionally. Every vote counts: recall the senatorial race in NH decided by 1 or 2 votes a few years ago, or (closer to where I now live) the East Palo Alto incorporation election, decided by 13 votes and still being challenged in the courts.

Another thing: mikemcl@nrl-csr (Mike McLaughlin) suggests

> The "receipt" would contain the date, time, machine number, serial
> number of the vote, and name the candidates and issues for or
> against whom/which I voted. It would NOT list my name.

No, but the poll watcher who saw you vote and wrote down the machine number and time of day next to your name wouldn't have much trouble matching the receipt, if you ever returned it.

I'm not saying that non-computerized systems are immune to error; but be careful that a technology that appears value-neutral (such as "representative random sampling") isn't ignoring political reality or creative dishonesty.

Computerized voting

<Polnicky%PCO@CISL-SERVICE-MULTICS.ARPA>
Thu, 6 Mar 86 08:11 MST

I find the various suggestions to back up computerized voting with physical ballotting as taking steps in the wrong direction. Certainly we can reduce risks by backing up computer/automated systems with human beings, where feasible, but to keep around a bunch of punched cards in order to ensure the integrity of electronic voting seems to me to be the wrong approach.

Larry Polnicky, Honeywell Information Systems, McLean, Virginia.

Computerized voting

Peter G. Neumann <Neumann@SRI-CSL.ARPA>
Thu 6 Mar 86 17:33:34-PST

This is not a VOTIVE message; I have broken my vow to remain silent while watching the schemes for voting integrity get wilder and less controllable. DEVOTED as I am, I can no longer keep silent. My main point here is that as more complex mechanisms are added to control or audit the integrity of the voting process, the more vulnerabilities are likely to be introduced, and the less controllable the whole process is likely to be. Nancy Leveson makes a similar point in her survey paper on software safety: as complexity is added to control safety, the more things get out of hand. I am prompted to drag out my old Albert Einstein quote -- for our newer readers:

> Everything should be made as simple as possible, but not simpler.

There is intrinsic complexity in the voting process. A voting scheme with no controls is easy to misuse. A voting scheme with many controls can also be misused, but in different ways -- perhaps requiring greater subtlety. Furthermore, such a computerized system must be used and administered by ordinary mortals; however, elaborate procedures tend to break down or be vulnerable. Furthermore, remember that many of the programs controlling elections are written by just a few software houses. The potential for Trojan-horsing around is enormous. A gifted system programmer can pull off all sorts of things. We have already seen cases of data changed on the fly in computer-counted ballots, even with consistency checks and audit trails (which themselves can be fudged). One can dream up all sorts of checks and balances -- formal verification of the algorithms, crypto seals on the stored code for integrity, encryption schemes to detect added ballots, and so on, but there are always points of vulnerability.

So, in the discussions here, please let us try to be realistic!

Peter

ATM Ripoff

Dave Curry <davy@purdue-ecn.ARPA>
Thu, 6 Mar 86 08:59:55 EST

WASHINGTON (UPI) - A computer glitch enabled a man to get away with $140,000 in $10- and $20-bills in a weekend run on 16 automatic teller machines in the nation's capital and its Virginia suburbs, the Secret Service said Wednesday.

Michael Caputo, 31, of Fairfax Station, Va., admitted in federal court Tuesday to using a stolen VISA credit card to make more than 400 withdrawals from the money machines last October.

The withdrawals represent the largest fraud committed agains VISA with an automatic teller machine, officials said.

"Why didn't someone else in line notice it?" asked John Magaw, a Secret Service agent. "It's very bizarre. All of a sudden this guy realized how good he had it. His pockets just weren't big enough. The machines just weren't programmed to stop."

Caputo was photographed by monitors at the 16 mechanized tellers receiving $300 during each transaction - at times smiling while other times holding bags of money.

"Normally, you can't take more than $200 at a time, and (most machines) will not allow you on nights and weekends to go beyond a certain limit," Magaw said. "Somehow, the safeguards broke down to allow for that to happen."

Magaw said that Caputo apparently used the VISA card at two banking institutions. He said that the two computers did not "blend together," and allowed him to take large amounts of money without being detected.

"It's like having a Chevrolet and a Buick and putting a carburetor from one on the other," Magaw explained. "You may get it to work, but it just doesn't quite go together. There's glitches that have to be worked out."

He emptied the machine of several thousand dollars, put it all into a paper bag, and left. The next day he went to the main office of the bank, saw the manager, and said, "Your teller machines can be robbed." The manager of course said this was impossible, at which point my friend dumped the bag of money on his desk and said, "You won't be wanting this back, then." The machines were down for the next several days...

Anybody have some stats on these things? I seem to recall seeing something that the banks are still losing money on them, but it didn't show any figures. Anyone have any data on this? I'm sure that given a few hours most people on this list could come up with at least one way to rob the machine down on the corner.... (let's not discuss the methods in detail though; I'm sure the banks have enough problems without us advertising ways to steal from them).

--Dave Curry

[I have various inside stories about the extent of fraud, but the victimized institutions seem to keep pretty quiet. They don't want to lose customer confidence and customers. Besides which, they can simply up the rates to amortize the losses. Who cares, especially if the customers don't even know? (OK. I care.) PGN]

Internet importance/robustness

Tom Perrine <tom@LOGICON.ARPA>
6 Mar 86 16:50 PST

The following message, which was in the tcp-ip list from SRI-NIC was in discussions of Internet (ARPA/MIL) Mailbridge performance. I think it is interesting from a RISKS point of view. How much does the computer science, aerospace, etc industry/research depend on the Internet?? What are the consequences of a long-term failure of ARPAnet? How suceptable is the ARPANET to terrorism/natural disaster/etc. ?

------BEGIN INCLUDED PORTIONS ------

>Date: 3 Mar 1986 17:03:11 EST
>From: Edward A. Cain <cain@EDN-UNIX.ARPA>
>Subject: Re: Mail Bridge Performance
>To: gross@mitre.ARPA (Phill Gross)
>
>Phill,
>
>Thanks for the summary of mailbridge traffic. I think it does partially
>explain why performance is so awful at times thru the mailbridges. The
>correlation with school schedules is interesting, too, and probably a better
>guess than any I've heard recently.
>
>There is one other important consideration. Performance on the ARPANET alone

```
 >has been terrible at times. For example, ICMP ECHO and ECHO REPLY round-trip
 >measurements between east and west coast hosts were averaging 18 seconds on
 >Feb 3-4, with tails of the delay distribution out to 37 seconds, as measured
 >from DCEC (via arpanet) and at BRL (via milnet). Delays were very high
 >again during the Feb 12-14 time period. Even worse, on Feb 20th, one hour
 >in the afternoon the roundtrip delay from DCEC to the arpanet interface of
 >the ISI mailbridge was 30-40 seconds, and from DCEC to the arpanet
 >interface of the SRI mailbridge the delays were 45-47 seconds during the
 >same hour, with 90% packet loss!!!
 >
 >Usually, this kind of behavior on the arpanet is coincident with the outage
 >of key lines or nodes in the arpanet. On Feb 20th for example, line 76
 >(utah to lbl2) and line 76 (sri2 to collins) were both down most of the
 >day because of flooded cableheads.!!! The loss of a key component in the
 >arpanet seems to create serious congestion when the traffic goes up. And
 >congestion is noticed quickly by the mailbridges, which are among the
 >busiest arpanet hosts in terms of both packets sent and connection blocks
 >used (in the IMP).
 >
[REST OF MESSAGE TRUNCATED]
 >Ed Cain


The recent message about flooded cableheads and the potential vulnerability
of the internet to loss of critical components made me wonder:

 How many IMPs are there on the ARPA side?              [Hundreds]

 How many on the MILNET side?                           [Hundreds]

 Where are they? I would assume that at least the MILNET IMPs are
 in secure areas.         [Not necessarily, but they are under the
                           control of DCA and BBN.  That helps.  PGN]

Tom Perrine
```

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 2: Issue 24

Saturday, 8 Mar 1986

Contents

Computerized ballot stuffing

ihnp4!ihuxn!agk@ucbvax.berkeley.edu <Andy Kegel>
Fri, 7 Mar 86 08:23:30 PST

In our area (extreme suburban Chicago, aka "the boonies"), we use a computer-counted paper-ballot voting mechanism. I am fairly sure I recall serial numbers on the ballots. However, I recognize that human memory is weak and subject to interpretation and assumptions. There is an election coming up this month, and I will be particularly careful to observe and understand the relevant facets of the process.

Remember, in Chicago, the rule is "Vote Early, Vote Often."

This message does not represent the position of my employer, or any individuals or organizations other than myself.

-andy kegel

Progress report on computerized voting

Kurt Hyde DTN 264-7759 MKO1-2/E02 <hyde%topcat.DEC@decwrl.DEC.COM>
Friday, 7 Mar 1986 05:57:00-PST

A sincere thank you to all the people who have responded to my request for assistance in computerized voting standards.

I called New Hampshire's Secretary of State and he will be meeting with me and some other people regarding security standards. I will be proposing something like the following:

> Computerized voting booths should print a paper ballot for each voter to view and check for accuracy. The hardcopy ballot must be visible to the voter by appearing under a covered (transparent) window. The dimensions of the window must allow for at least 10 votes to be viewed at one time. The printer must then feed each ballot into a ballot box which is guarded from access outside access while the voting machine is in use. The audible signal which confirms that the voter is completed may occur after the hardcopy of the ballot is no longer in view.
>
> In order to protect the anonymity of the voter casting each ballot, each ballot must be on a separate piece of paper when deposited in the ballot box. It may be be cut after printing or be sheet-fed into the printer.
>
> This additional functionality allows for a recount. The current machines do not have the capability of recounting the ballots. They only have the capability to recalculate from subtotals.
>
> Because of recount capability, it will be possible to resolve election disputes at the place of the voting. This means it will not be necessary to contact the FEC and National Bureau of Standards in order to perform an audit on the machine's computer programs. The procedure for the FEC and NBS to audit the machine's computer programs has not been established and is likely to be extremely complex as certainly procedures must be established to be certain that the computer programs haven't been tampered with in order to return them back to their proper state.

My students at Rivier College will still be investigating further into the proper security controls. One of them is considering a way to let the voter see his/her ballot and abort that ballot. The printer would then print an appropriate message such as "CANCELLED" on the bottom.

Once again, let me thank all those who are participating. Your assistance is very valuable and appreciated. Let us not let the United States suffer from a similar disaster as the Phillipines.

Kurt

Wild Modems

Bjorn Benson <sun!fluke!uw-beaver!entropy!dataio!bjorn@ucbvax.berkeley.edu>
Wed, 5 Mar 86 16:50:59 pst

All this talk in RISKS about modems calling humans rather than computers reminded me of an article I read about telecomputing in Europe: it seems that laws in Europe require modems to have equipment attached to explain what is going on in four languages, should the computer happen to dial a wrong number.

Bjorn N Benson

Re: Misdirected modems

Phil Ngai <amdcad!phil@decwrl.DEC.COM>
Sat, 8 Mar 86 00:34:30 pst

This is an often repeated wives tale by people who ought to know better. With ordinary dialup modems of the 103/212 class, it is the *answering* modem which initiates a tone. The originating modem (the one that dialed) remains silent until it hears the carrier of the answering modem.

Thus, if a computer dialed a wrong number, the person receiving the call would hear nothing, not a "funny whistle".

power outages

Phil Ngai <amdcad!phil@decwrl.DEC.COM>
Sat, 8 Mar 86 00:46:23 pst

I am familiar with AMD's data center. It is relatively small by comparison to some sites, having only four IBM 3081s and one 3090, but it does have battery backup and a huge dual turbo charged diesel generator. The diesel has a thousand gallon fuel tank, which will last it 24 hours. We have arrangements to get refills within that 24 hour period, so our data center could presumably survive an indefinite outage and you could continue to order chips from us even during a blackout!

Earthquake problems with Nuclear Reactors.

"Lindsay F. Marshall" <ncx%cheviot.newcastle.ac.uk@cs.ucl.ac.uk>
Fri, 7 Mar 86 10:20:51 gmt

This is not really computer related, but seems interesting all the same....

A recent article in The Guardian highlighted some investigations into the safety of British nuclear reactors in the face of the kind of mild earthquakes that we have here. In particular it mentioned the Calder Hall reactor which is nearly 25 years old and is built quite near to the area of Britain that has the most earth tremors. This installation has a reactor vessel weighing 2000 tons suspended 18ft above the ground which is now so radioactive that it would be impossible to examine or modify. The investigation showed that the original safety calculations "had been done on the back of an envelope" and that the reactor bolts might shear with an earthquake of 0.5 (units?). There was an earthquake of that intensity last year, but it is impossible to find out if anything was damaged because of the intensity of the radiation not forgetting the 5ft of concrete and steel surrounding the chamber.......

So if you hear that Newcastle vanished, you'll know why!

[and we'll be back to carrying coals ... PGN]

Search RISKS using swish-e

Report problems with the web pages to the maintainer

THE RISKS DIGEST

Forum on Risks to the Public in Computers and Related Systems

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

Volume 2: Issue 25

Monday, 10 Mar 1986

Contents

Balloting

Barbara E. Rice <rice@nrl-csr>
Mon, 10 Mar 86 12:43:50 est

There has been much discussion on the net as to the secrecy of ballots. No one has mentioned yet the situation I find myself in regularly with the absentee ballot system. My name is printed on the outside of the envelope and I assume checked off when it arrives at its destination to insure that I don't vote 2 or more times. What is to prevent someone from just taking a peek and seeing who I voted for. In fact I have never heard what the method is to insure that my name and who I vote for are not put together. There is a simple way to check this out to see if my vote is secret but I do not have the courage to try it. All I would need to do is vote a straight communist ticket. If my security clearence is revoked in the next six months it would be safe to assume my vote is not secret. Anyone know of a non-career threatening way to check this out?
Barb R.

Canceling ballots

"Jim McGrath" <MCGRATH%OZ.AI.MIT.EDU@XX.LCS.MIT.EDU>
Mon 10 Mar 86 22:12:18-EST

```
 Subject: Progress report on computerized voting
   From: hyde%topcat.DEC@decwrl.DEC.COM  (Kurt Hyde DTN 264-7759 MKO1-2/E02)
   My students at Rivier College will still be investigating further
   into the proper security controls.  One of them is considering a
   way to let the voter see his/her ballot and abort that ballot.
   The printer would then print an appropriate message such as
   "CANCELED" on the bottom.
```

I can see a lot of potential problems with canceling already printed ballots. In particular, any technology that takes a ballot which would, by default, be valid and then modifies it to be invalid could be used to invalidate valid ballots after the polls have been closed. Moreover, if the technology fit in a voting booth, then it is probably portable enough so that such modifications could be done on site (i.e. without physically removing the ballots to an unauthorized location).

I would thus suggest that you use some sort of display (CRT, LED, or just light bulbs next to the appropriate names) for voter confirmation. Failing that, you should print out the ballot as before, but on white (say) paper. If the voter confirms the ballot, then the white copy is stamped CANCELED, a duplicate is printed on red (say) paper, and both are deposited in separate boxes. While both copies would be kept, only the red copy would be treated as authoritative.

You can still forge red ballots (you can forge any paper ballots). But you cannot turn a red ballot into a white one by using a CANCEL stamp or somesuch. Only gross mutilation or removal of the ballot from an authorized area could cancel the valid ballot - both harder to do (at least undetected).

Jim

bank robbery

<ulysses!burl!rcj@ucbvax.berkeley.edu>
Sat, 8 Mar 86 20:45:11 est

I read an excellent book a few years ago simply entitled "Computer Crime".
                                   [PRESUMABLY BY DONN PARKER? PGN]
I highly recommend it to the readers of mod.risks. Here are a couple of example horror stories from the book (from memory, sorry):

a) A guy gets a bank loan, when he gets his payment book he sends in the *last* payment slip from the book with his first payment. The bank's

computer sends him a cheerful letter congratulating him on settling his
debt in a timely manner.

b) A guy opens an account at a major NYC bank with several thousand dollars. After he gets his personalized checks, he goes to a shady printer friend and has the guy print up identical checks but with a bogus magnetic number on the bottom. He then goes on a $1,000,000 check-writing spree. Every time on large purchases they call his bank and electronically verify that he can cover the check. Every time the sorting machine at the bank sees the leading ?3?-digit code of a West Coast bank, and automatically mails the check there. The West Coast bank's sorter kicks the check out to manual sorting because it has a bogus account number. The human sorter takes one look at the check and sees the name of the NYC bank and blithely mails it back... They finally got onto him when one of the checks had been through so many sorter and mailer machines it was nearly in shreds, and the human sorter on the West Coast got curious enough to look at the magnetic ink number.

c) Guy opens an account in a Washington, D.C. bank. He rips off several pads of blank deposit slips from the lobby of said bank, takes them to a location (?maybe he worked at the place?) that has a magnetic ink typewriter. He laboriously types his own account number on the bottom of all the slips, then places the pads back in the lobby of the bank. A month later he withdraws $100,000 and disappears.

The MAD Programmer -- 919-228-3313 (Cornet 291)
alias: Curtis Jackson ...![ihnp4 ulysses cbosgd mgnetp]!burl!rcj
...![ihnp4 cbosgd akgua masscomp]!clyde!rcj

[OLD STUFF, BUT WHY NOT? WE HAVEN'T HAD THEM HERE BEFORE. PGN]

Re: Earthquake problems with Nuclear Reactors

<mcnc!rti-sel!dg_rtp!throopw@seismo.CSS.GOV>
Mon, 10 Mar 86 17:33:22 est

> From: "Lindsay F. Marshall" <ncx%cheviot.newcastle.ac.uk@cs.ucl.ac.uk>
> Subject: Earthquake problems with Nuclear Reactors.
> [...]
> So if you hear that Newcastle vanished, you'll know why!
> [and we'll be back to carrying coals ... PGN]

Ok, ok, cute, I laughed, I liked it. But nuclear paranoia being what it is, and with no smiley, this seems to me to be blatantly inaccurate, and worthy of clarification. As far as I know, nothing short of refining the fuel and making a bomb out of it can cause a power reactor to explode with a large yield. Or perhaps the two of you know of some other way that a power reactor can cause a city to "vanish" (implying a sudden, physical removal of the city from existence or perception)?

[Whatever happened to Sverdlovsk -- or was that biological? PGN]

103/212 modems DON'T WORK AS SUPPOSED (10% of the time?)

Brent Chapman <chapman%miro@BERKELEY.EDU>
Sun, 9 Mar 86 02:00:47 PST

In article <8603081745.AA20185@ucbvax.berkeley.edu> Phil Ngai writes:
 >RISKS-LIST: RISKS-FORUM Digest, Saturday, 8 Mar 1986 Volume 2 : Issue 24
 >
 >Date: Sat, 8 Mar 86 00:34:30 pst
 >From: amdcad!phil@decwrl.DEC.COM (Phil Ngai)
 >To: risks@sri-csl.ARPA
 >Subject: Re: Misdirected modems
 >
 >This is an often repeated wives tale by people who ought to know better.
 >With ordinary dialup modems of the 103/212 class, it is the *answering*
 >modem which initiates a tone. The originating modem (the one that dialed)
 >remains silent until it hears the carrier of the answering modem.
 >
 >Thus, if a computer dialed a wrong number, the person receiving
 >the call would hear nothing, not a "funny whistle".

Sorry, maybe that's how it's SUPPOSED to work, but it just doesn't happen that way. I work with several 103/212 class modems, and every one of them, at least 10% of the time, "responds" to a "carrier" before there actually is one. There appear to be no fixed, recognizable reasons for this. They will respond to rings, busy signals, or someone picking up the line. All of these modems are recent models, purchased within the last year, so I don't think it's a problem of out-of-date technology.

Brent Chapman
chapman@miro.berkeley.edu
ucbvax!miro!chapman

Re: misdirected modems

"MARTIN J. MOORE" <mooremj@eglin-vax>
0 0 00:00:00 CDT

> From: amdcad!phil@decwrl.DEC.COM (Phil Ngai)
> This is an often repeated wives tale by people who ought to know better.
> With ordinary dialup modems of the 103/212 class, it is the *answering*
> modem which initiates a tone. The originating modem (the one that dialed)
> remains silent until it hears the carrier of the answering modem.
> Thus, if a computer dialed a wrong number, the person receiving
> the call would hear nothing, not a "funny whistle".

True, the answering modem normally initiates a tone first. However, some 103/212-class modems (e.g., the Hayes Smartmodem 1200 which I use at the office and the similar Prometheus P1200A which I use at home) will start a tone after a few seconds regardless of whether the answering modem starts one. I have the speaker on during the dialing and connection process, and both modems always start a tone whenever a call fails to go through or gets a wrong number

(one or the other happens about 10% of the time.) Anyone who is skeptical of
this is welcome to drop by my office and I'll be happy to demonstrate it.
In fact, I whistled at some poor soul on a wrong number while dialing in for
this terminal session!

marty moore (mooremj@eglin-vax.arpa)

Re: misdirected modems

Phil Ngai <amdcad!phil@decwrl.DEC.COM>
Mon, 10 Mar 86 17:42:34 pst

I have a Hayes and I just tried it and it does not
whistle at me.

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 2: Issue 26

Friday, 14 Mar 1986

Contents

Integrity of the Electoral Process

<MJackson.Wbst@Xerox.COM>
12 Mar 86 11:39:29 EST (Wednesday)

It seems to me that the discussion has strayed from the mark. No balloting procedure is completely unbreakable. Current systems appear to be reasonably secure, but this is primarily due to effective vigilance (e.g. poll watchers from each party). When enough of the "system" falls under the effective control of a single organization then fraud becomes possible, hence inevitable (e.g. Chicago under the Machine).

The "risk" involved in computerization of the ballot collection and counting process is the centralization of much of the process under the control of a single organization (hardware and software system). The challenge is to assure that the resulting system is sufficiently distributed and subject to routine checks so that the potential for fraud is not increased.

Apropos of this, it is not clear to me that the proposal for printing individual ballot hardcopies addresses what would otherwise be an *increased* risk. For example, with lever-type voting machines is some record kept beyond the candidate tallies read out when the polls close?

Mark

[Apparently no individual record is kept -- only the running totals. Fraud-prevention is largely dependent on the poll watchers. But it may be relatively easy to vote twice in a large and noisy room if your machine is facing away from the poll watchers back-to-back with another machine facing the other way -- unless the system is set up so that it has to be rearmed manually each time the exit-lever automatic vote recorder is triggered.

There are always some vulnerabilities, as I noted in RISKS-2.23, including bribed officials. The recent election in the Philippines give us another datapoint. PGN]

Ballot Secrecy

"Lindsay F. Marshall" <ncx%cheviot.newcastle.ac.uk@cs.ucl.ac.uk>
Wed, 12 Mar 86 11:28:38 gmt

One of my regular grouses to Clerks at election time is that the Ballot is not actual secret. They always say "oh yes it is", but when you point out that each voting slip is stamped with a serial number (when you get the paper) which is recorded in such a way that it can be traced back to you, they then say "Oh, but that's in case there is any Ballot Rigging so that we can backtrack to find multiple votes etc.". The ballot in UK elections is most definitely not "secret" in the sense that most people assume, though there is no evidence that anyone is checking out how you voted (yet).

Nuclear waste-land

Jerry Mungle <JMUNGLE@USC-ISIF.ARPA>
11 Mar 1986 06:26:43 PST

Re: Nuclear power plant accidents...

The explosion in the USSR was due to storage of nuclear waste, not a power plant accident. However, seems I recall there are some low probability (aren`t they all) accidents which can send a breeder reactor into a low yield explosion (probably *very* dirty, too).

Two tangental comments - I live near TVA's Browns Ferry reactors. ALL of the operators failed NRC license tests(!) so BF has been shut down till 80% can pass. Is there a license for reactor control software, and if not, perhaps TVA might be a good place to test (worst case operator actions and all that)?

Second, there is a siren to alert the population to a BF accident with a leak. Nearby is a state prison with an occasional leak. People have suggested a siren to warn of escapes, but the chance for confusion is high. Anyone know of a good way to spread an alarm when you have multiple risks??

(ps. smiley face to the TVA test suggestion....)

Nuclear disasters

"Lindsay F. Marshall" <ncx%cheviot.newcastle.ac.uk@cs.ucl.ac.uk>
Wed, 12 Mar 86 11:24:01 gmt

The last line was a joke - the problem with 2000ton reactor vessels dropping 18ft is not explosion but one of contamination. The radiation leakage would be huge and most of the South of Scotland and North of England would be affected. If it actually happened Newcastle might just as well have vanished......

103/212 modems [Will the messages never cease?]

<ucdavis!lll-crg!seismo!harvard!encore!vaxine!wanginst!wang!ephraim@ucbvax.berkeley.edu>
Tue, 11 Mar 86 18:27:52 est

In RISKS-2.24, Phil Ngai writes:
> This is an often repeated wives tale by people who ought to know better...

As it happens, I can testify that Phil's statement is not correct, or at least not universally so. On Sunday 3/9, I called the modem line of a friend using my Applemodem 1200. His modem was not ready, so he answered the call manually and said "hello" to get my attention. He tells me that my modem *did* produce carrier when he picked up the phone.

Sorry, Phil.

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 2: Issue 27

Saturday, 15 Mar 1986

Contents

Overload of a different sort [Air traffic stoppage]

<TMPLee@DOCKMASTER.ARPA>
Fri, 14 Mar 86 12:26 EST

This may or may not involve a computer, but I think it did. Those of you travelling in the Southeast yesterday were made well aware that the Atlanta airport was thrown into a complete chaos by the thunderstorms in the area, and this rippled throughout the air transport system. To make a long story short, I managed to get out of Augusta on a plane that was five hours late, which was okay since that had me leaving Augusta only two hours after I was supposed two, and my connecting flight was also two hours late. The computer part is this. After we boarded in Atlanta the pilot announced he had called for his air traffic control clearance and was told that flow control into Minneapolis was in effect and there would be an indefinite delay. Those of you who have had nothing to do with air traffic control may not realize that in the late 60's or early 70's a change was made in the way the over-all air traffic was controlled: instead of stacking planes up over destinations when traffic got crowded, a national system was instituted to monitor and control the general flow, not allowing a plane to depart until there was a clear slot for it to land in. This is all coordinated between the terminal air traffic control computers and a central computer in Washington. Anyway, we sat for about another half hour and the pilot called again. Same answer. He and/or the Delta operations people used a little common sense: the weather in Minneapolis was just fine and they could understand no reason why the airport should be congested -- they called Washington and after someone checked around received the answer "there shouldn't be any flow control into Minnapolis; someone got their wires crossed." We left in five minutes, having been on the ground for nearly an hour by either a computer error or human error only possible because the computers were installed to manage a humanly unmanageable task -- almost certainly the error was caused by the overload generated to handle the disrupted schedules throughout the system.

Ted

Cordless Phones Cry Wolf!

Peter G. Neumann <Neumann@SRI-CSL.ARPA>
Sat 15 Mar 86 12:00:04-PST

The SF Chronicle 15 March 1986 has a news story about cordless phones making ``ghost'' phone calls to the emergency number 911 (and presumably to other numbers as well). The cordless phones, which send out and respond to radio frequencies, behave strangely when their batteries start to run down. In addition, other household appliances can spur cordless phones to start diaing spontaneously. Michael Moos (president of the National Emergency Number Association) was quoted: ``Frequencies given off by other appliances -- micorwave ovens, blenders and even fluorescent lights -- interfere with the cordless phones and make them start dialing.'' On an average day, at least 12 of the 2000 calls received by Santa Clara County's 911 system are such ghost calls. [Cf. heart pacemaker interference, Sputnik triggering garage door openers, automotive CB interference, etc., in past RISKS.] PGN

The Mob Breaks into the Information Age

Mike McLaughlin <mikemcl@nrl-csr>
Fri, 14 Mar 86 15:17:48 est

INFOSYSTEMS, Vol 33, No. 3, March 86 carries subject article, beginning on page 40. Also several other computer security items. Ought to help sell a few password systems, at least. - Mike McLaughlin

[Non]computerized train wreck

<ihnp4!utzoo!dciem!msb@seismo.CSS.GOV>
Fri, 14 Mar 86 08:45:38 EST

The wreck of a VIA Rail Canada train and Canadian National freight
train on February 8 was mentioned in this forum.
    [See Martin Minow, RISKS-2.9; Chuck Weinstock, RISKS-2.12]
I think it's worth pointing out that the accident has been attributed
to human error, specifically by the CN engine crew, both of whom were
among the 23 killed. (Not 30+ as feared originally.) They drove past
a stop signal which both men should have seen.

Not only was this NOT a case of computer malfunction, but indeed, a more
fully computerized system (with cab signalling and automatic train stopping)
would probably have prevented the accident.

Mark Brader

[A fine example of the risks having to include people, not just
computers, and of a more pervasive role of the computer than meets
the eye -- indeed a more human-oriented computer system might have
helped! Thus, even though it appears NOT to be a computer problem,
we discover that the computer could have done better! But, of course,
don't blame the computer system. Blame the people who specified,
designed, and implemented it -- not JUST the train operator(s). PGN]

Ballot Integrity; Specialization in Decision-Making

Tom Benson 238-5277 <<T3B%PSUVM.BITNET@WISCVM.WISC.EDU<>
Fri, 14 Mar 86 10:54 EST

I don't want to extend this discussion of ballot integrity, but my
understanding is that in Pennsylvania there is a registration number
on the ballot when it is given to the voter, but the voter tears it
off and retains it, so the ballot when in the ballot box is not
traceable to the voter.

I'm curious about the tone of some of the discussion on this issue.
Granted we shouldn't assume the absolute integrity of non-computerized
voting without careful scrutiny. But some of the contributions seem, if
I am not mistaken, to justify computerized balloting on the grounds of
a broad (and unarguable) assumption that "any balloting process can be
subverted." Sure. But the object is to insure insofar as possible that
it won't be, and that means, primarily, protecting (1) secrecy, and
(2) accuracy.

Does anyone have an opinion on the question of how the local situation,
in this case RISKS, may influence the general consideration of the issue?
That is, RISKS is devoted to an interest in computers, not voting. Does
that, explicitly or implicitly, influence the question of what ought to
be relevant to the decision process? I'm not complaining, nor am I
criticizing previous comments by correspondents or the editor. What I am
trying to do is draw attention, as a communication scholar, to another

potential RISK: the use of electronic mail and digests with clear agendas may inhibit the generalism needed to address substantive problems. Does anyone have instances of this in their experience? (Note: I understand that the problem is not limited to computers; committee work in general suffers from this problem).

Tom Benson T3B AT PSUVM (BITNET)

[Hmm. For some reason I am rarely accused of undergeneralizing. I keep mumbling that to deal with RISKS, we must do so holistically, and that the computer is only a small part of what must concern us -- even though it is the primary justification for the existence of this forum. Any weak link can be devastating. RISKS indeed tends more toward breadth than depth, toward ALL RISKS than just computer risks. Indeed a few other people have commented that we have strayed off into the subjects of THEIR on-line forums! I don't really think there is too much danger that we are too narrow. But discussion is welcome if relevant to RISKS. PGN]

Network Security, Integrity, and "Importance"

"Kurt F. Sauer" <ks%a.cs.okstate.edu@CSNET-RELAY.ARPA>
Fri, 14 Mar 86 18:46:51 CST

Tom's Perrine's question about the Interface Message Processors' (IMP) security [RISKS-2.23] is a really well-founded one. As I see it (and I haven't spent much time thinking about it, really), we can design a network's security procedures based on some information and management judgements.

Try answering some of these questions about the network you manage or administer:

o How critical is the general network operation?

This can be based on many things, not the least of which include the value of the tokens passed on the network and the desirability or necessity of proper message reception.

o How confidential are the messages? Are patterns, themselves, classified?

Traditional cryptology can be applied to "entire messages" (or whatever the DIRNSA will let you get away with), but would releasable routings disclose critical paths? Would they "give away" operational information which should be protected?

o Can message speed be increased for vital information whose delivery is paramount? I'm not sure that this is as much a security problem as it is a basic applied-computer-science question. Some feel that packet precedence systems are unnecessary; some feel otherwise.

The Defense Data Network (DDN), which is comprised of the ARPAnet and the MILNET, serves a mighty diverse consumer market. Universities, research facilities, commercial institutions, and government operations all share the facilities of the network.

Currently, some classified (i.e. sensitive) operations make use of the DDN. Systems like the COINS-CINCPAC project now use the DDN as a transport medium; loss of the medium would have at least some impact on CINCPAC's intelligence operations. For such setups, the basic network security is ensured through fail-secure cryptographic setups which are only able to prepend one specific message header to an already encrypted packet. (One thus gets around the red-black interface problem with packet addressing.) And physical security is ensured by using guards, locked doors, and the like at the point of security interface, and at all secured locations.

But this doesn't address the Internet physical or electronic security in general. I believe that the Defense Data Network Program Plan has a scheduled dis-integration of the DDN parts very soon. Obviously we have already traversed the ARPA/MIL separation, but more is soon to come. With the introduction of Internet Private Line Interfaces (IPLIs) (and, based on various community needs, estimates for numbers of IPLIs are nearly 1000--and probably higher), the network can divide itself such that hosts will not talk to non-community-of-interest hosts. The "big plan" includes folding MINET, MILNET, SACDIN (!), and IDHS (!!) into one network: the DDN. The current ARPAnet will remain an R&D network, essentially isolated completely from the DDN.

I haven't been watching the network events (due to my absence) for about a year now, so I don't know how far along we are in this plan. But if it's implemented (we're all waiting for BLACKER, so budgetary holdbacks may well intervene), then "vital network nodes" would be physically secured, with the ability to fold ARPAnet into DDN in the event of a crisis where additional redundancy is required to limit network failures due to attacks on the system.

Perhaps someone who really knows a lot about these things could comment on the physical security side of the DDN house. For those of you who are interested, I have some citations to references which I would be happy to share with persons on the ARPANET or MILNET; I will respond only to e-mail requests.

Kurt F. Sauer
Tulsa, Oklahoma

Internet: ks@a.cs.okstate.EDU UUCP: ks@svo.UUCP

Modems [still... enough already?]

James R. McGowan <jrm@Ford-wdl1.ARPA>
Fri, 14 Mar 86 16:48:27 PST

In re the modem controversy: the originating modem contains circuitry

to detect answering tones (in the range of 2000-2400 Hz.) It should
remain silent until it does detect the answering carrier (at least
if the modem claims to be Hayes standard.) However, other sounds on the
telephone line (noise, human voice, even just picking up the phone)
can sometimes excite th detection circuitry and software, resulting
in the originating modem turning on its tone generator. Sorry, but
Phil does know what he's talking about.

Jim McGowan
(jrm@ford-wdl1)

[Let's BLOW the WHISTLE on this one. There's no modem operandi. PGN]

Search RISKS using swish-e

Search RISKS using swish-e

THE RISKS DIGEST

Forum on Risks to the Public in Computers and Related Systems

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

Volume 2: Issue 28

Monday, 17 Mar 1986

Contents

Risks of commission vs. risks of omission

Peter G. Neumann <Neumann@SRI-CSL.ARPA>
Sat, 15 Mar 86 17:30:09 pst

Dave Parnas in a private note to me has raised a set of concerns involving the actions and inactions of a particular system. Those concerns seem very important to RISKS, and so I quote him here (with his permission).

> "What about the difference between risks of commission and risks of omission? Whenever we speak of a risk it is shorthand for the risk of some specific danger. I consider a risk to be one one of commission if the danger is that the system will perform some action from a finite set of "bad" things. A risk is one of omission if the danger is that the system does not perform the task that it was built to perform. I think risks of commission are less difficult to deal with than risks of omission for two reasons: (1) for risks of commission one can do specific "backward" analysis to look for ways that that danger could occur, (2) for risks of commission one can include checks and hardware to prevent the danger. Risks of omission are often insurmountable because confidence that they will not

occur requires a proof of "correctness" or at least a proof of certain aspects of correctness. Do the readers of the forum agree with this distinction and evaluation? Can they site save examples of successful software with a severe risk of the omission type?" [Dave Parnas]

There are several comments that I would like to make, and then I'll turn this open to the Forum.

The finite set of "bad" things may be incomplete. An example in the security community is the multilevel security property -- NO FLOW of information downward to a lower level of security or laterally to another compartment at the same security level. This is the property upon which various security kernels are based. However, it represents only a portion of the "bad things" that must be prevented. Furthermore, proving the NO FLOW property for a few dozen kernel functions is not enough if the entire machine language is accessible via assembly language!

Yes, the former may seem easier to deal with -- at least superficially. However, the errors of commission are insidious in that it is very hard to GUARANTEE their absence. In many cases the set of properties ("bad things") is already stated negatively ("X MAY NOT HAPPEN", as in the case of the NO FLOW property), and applies only abstractly. Even even if you can demonstrate that a particular interface (e.g.,a security kernel) satisfies the desired set of properties (that is, the design satisfies the properties and the code and hardware together are consistent with the design), the set of properties may incomplete. Thus, "correctness" arguments are relevant in the errors of commission as well -- down to and including the hardware.

Dave reminds us of Martin Moore's example of the range safety shuttle destruct system.

"Here there are risks of both kinds. There is a risk that the system may destroy a shuttle that performs properly. There is also a risk that it may not destroy a shot that should be destroyed because it is about to crash in Miami's heavily populated area. Martin described how many measures could be taken to make the commission risk less likely. Physical control of data paths was one of those measures. However, it is much harder to see how we can make sure that the destruct system will perform. We would need some correctness arguments or extensive testing to have faith that it would perform when it should." [Dave Parnas]

The risks of omission are also insidious in that the model of what must be done may be incomplete. While the distinction between errors of commission and omission is valuable, I suspect that there are essentially equivalent problems with each, but this is probably of little help in practice. Both types of risks must be considered. Furthermore, in some cases, a given problem may involve both types of errors.

Peter

[Perhaps a survey of the disaster list (e.g., RISKS-2.1) might be in order, but I want to get this issue out without further delay. PGN]

The TIME is RIPE -- a clock problem

Peter G. Neumann <Neumann@SRI-CSL.ARPA>
Fri 7 Dec 84 09:46:27-PST [WRONG!]

MORE LIKE Mon 14 Mar 7:50AM PST]

Somehow the time-of-date clock on my system got reset to 7 Dec 1984 last night around 10:40 PM PST, while I was logged in. I was apparently the only user on the system at the time, but I was doing nothing unusual. Could it have been a dropped bit (despite parity) (I haven't had the patience to do the calculation of the time difference)? or a time-dependent software glitch? At any rate, it is something I had never seen before, and it seems quite relevant to RISKS.

The side-effects of such a clock burp could be very painful. (1) A delete-by-date of older-dated versions of a file results in deletion of the newest versions actually created. (2) All of the messages in my mailboxes were marked as UNSEEN. In a mailbox with hundreds of messages, that is a nuisance. (3) In clock-dependent asynchronous systems, all hell could break loose. (Recall the first shuttle launch delay.) (4) All sorts of other things might stop working. (I wonder if anyone ever runs a system in the virtual past in order to keep the SCRIBE time-bomb from going off, to avoid paying UNILOGIC for another year!) PGN]

[I waited to send this issue out until the clock had been corrected,
in order to minimize further side-effects, notably confusion.]

Peter

Mailer Gone Mad?

<Landrum @ DDN1.ARPA>
14 Mar 86 14:12 EST

Comment: Found this in my mailbox. Something appears to have gone awry!!

Taylor Landrum
Forwarded message:

Date: Thu 6 Mar 86 22:27:50-PST
From: RISKS @ SRI-CSL.ARPA
Subject: RISKS-2.23
Sender: NEUMANN@SRI-CSL.ARPA
cc:
Text: LTC Elderd,

I just got another issue of Bar Code News in the mail, and it had an insert on something called "ID EXPO", which is sponsored by Bar Code News, and is billed as "the conference and exposition of automatic identification and keyless data entry". It will be held at the civic auditorium/Brooks Hall in San Francisco, 19-21 May.

...

- Jim Jack

-------------END OF FORWARDED MESSAGE(S)-------------

[I omit the rest of the message, and hope that Jim Jack does not mind my including this here. I hope you see that someone's mailer has committed A MONSTROUS SCREW-UP. The header information is precisely that of RISKS-2.23, and Landrum@DDN1 was on the list to receive that issue. But it is clear that the message received was truncated after some of the header stuff (notice the TO: field is missing!) and the text of another message concatenated. PGN]

Money Talks

<Matthew_Kruk%UBC.MAILNET@MIT-MULTICS.ARPA>
Sun, 16 Mar 86 15:43:34 PST

The following article appeared in the Vancouver Sun (Vancouver, B.C.), Saturday, March 15th:

New bills will prove that money can talk

OTTAWA - It costs six cents to make, wears out in about a year, and is an oddball in the U.S., where today it's only worth $1.43.

Someday it will even be able to talk - in both offical languages.

It's the new Canadian $2 bill, announced today by the Bank of Canada, which has redesigned the deuce - and its $5 pal - for introduction later this year.
...
The new bills will also have a feature to assist the visually-impaired distinguish denominations.

Don Bennett, a spokeman for the Bank of Canada, said the new bills will have a code printed into them which, when inserted into an electronic device, will activate a synthesized "voice" which will speak the denomination.

Bennett said the bank is continuing development work on the device, but field tests, which included Vancouver, were recently completed.

Bennett said it will be the end of the decade before the devices are in wide-spread use although some may be available by 1987. The target cost is below $50.
...

My curiousity is how "fool-proof" are these codes (I have not seen what the codes look like but I suspect something similar to that imprinted on personal checks) and devices. Does anyone know of something similar? Will money not only "talk" but "lie" too?

[I am reminded of the BART and METRO fare cards. Although the remaining fare is encrypted, the magnetic stripe is trivial to copy. Since the encoded signature of the $2 bill will be identical for all $2 bills, in principle it should be easy to copy -- perhaps onto an OLD $1 that has no such markings, although that is not such a great loss. What about higher denominations? (Holograms embedded in the bill to prevent forgeries (as in credit cards) would not help the blind much.) If you were blind, would you have any confidence in a machine that tells you that the bill you have just been given by a well-known shyster is a perfectly good $1000 bill? PGN]

Another discourteous modem

Glenn Hyatt <hyatt@dewey.udel.EDU>
Sat, 15 Mar 86 17:03:51 EST

The other day, someone finally reached me who had been trying for several days. I have a second phone line into my house that I use only for data -- no telephone attached -- and it seems she had gotten that phone number instead of the one I always use for voice. Usually I am either using the data line or the modem is turned off, so she kept getting a busy signal or no answer. Once, though, someone -- my modem, left on for once -- answered. It beeped, so she left a message, taking it for an answering machine. Took me for the sort who never returns phone calls.

Will the modem discussions ever hang up?

Rob Austein <SRA@XX.LCS.MIT.EDU>
Sat, 15 Mar 1986 19:19 EST

Peter,

I suggest that if you are as tired of modem stuff as you sound, you just redirect anybody who wants to talk further to TELECOM@XX. Lag time to the various parts of the net is bad enough that you will still be getting this crud for weeks if you don't put a lid on it.

--Rob

[I'm not tired of the topic itself, but I think our readers may grow a little weary of the seemingly endless variations on the theme. However, I think I may turn up my REJECT RATIO a little more. 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 2: Issue 29

Monday, 17 Mar 1986

Contents

Commission vs. Omission

"MARTIN J. MOORE" <mooremj@eglin-vax>
0 0 00:00:00 CDT

Dave Parnas's points regarding the shuttle destruct system are well taken.
The policy, stated informally, was that "it better work if we need it --
but it absolutely better NOT 'work' when we DON'T need it" which generated the
extreme emphasis on preventing what Dave calls "risks of commission." I feel
that the risk of commission on the destruct system is extremely small, while
the risk of omission is somewhat higher, although still small. During
validation testing and in every pre-launch checkout, we performed "exhaustive"
checks -- "exhaustive" meaning that we tried every combination of

```
  [(2 central computers) * (6 remote sites) * (2 computers per site)
     * (2 transmitters per site) * (2 comm paths to each site)
     * (2 possible commands in various sequences)].
```

Yeah, this takes a *LONG* time (with practice, we got it down to several hours if everything went smooth.) On one occasion during validation testing, we did find a software error which only manifested on a particular (central computer/comm path/remote computer/unusual command sequence) combination. Exhaustive tests *are* necessary.

I have often wondered why the emphasis was to prevent errors of commission over errors of omission (not to say that we wanted either kind, but errors of commission were definitely considered to be worse!). An erroneous destruct would cost the lives of the flight crew, loss of the Orbiter, and possibly damage on the ground if it occurred early in the flight (e.g., windows blown out, etc.) An erroneous non-destruct, in the worst case (if the ET were to detonate near the crowded spectator area on the NASA causeway), could cause the loss of TENS OF THOUSANDS of lives. Certainly this is worse than an erroneous destruct. I believe there may be a subconscious feeling that an erroneous destruct means the difference between a success and a disaster, while an erroneous non-destruct means the difference between a disaster and a worse disaster. Subjectively, that difference is not as great as the first, although objectively it may be much greater.

Martin Moore

<The usual disclaimers. I'm too tired to type in the whole silly thing.>

[By the way, Dave Parnas suggested the following example to illustrate his message in RISKS-2.28:]

"Consider elevators. Consider how much easier it is to prevent the floor indicator from saying "13" than to assure that the floor indicator will always give the actual floor that the elevator is on. The risk of indicating "13" can be gotten acceptably low by eliminating "13" from the set of indicator lights. The risk of indicating an incorrect floor or not indicating the current floor is much harder to eliminate." [Dave Parnas]

A Stitch in Time

<JAGAN@SRI-CSL.ARPA>
Mon 17 Mar 86 11:43:53-PST

[As it now turns out, the reboot occurred just moments BEFORE I logged in Sunday night. Here are some further details. PGN]

This is the probable sequence of events that led us back in time on CSLA:
1. A power glitch (late night SUNDAY) caused the F4 to hard boot.
2. During a hard boot, the TIME is retrieved from eleven independent sources (which are assumed to be correct!)
3. One of these sources had the incorrect time of some warm day in 1972 causing the average to be wrongly computed resulting in Dec 6th/1985.

Suggestion:
1. Change the statistical measure from MEAN to something less sensitive to one or two abnormal times; for example the average of the 5th, 6th, and 7th

largest times.

[IT IS ABSOLUTELY INCREDIBLE THAT UNSAFE ALGORITHMS continue to be used. This problem is as old as the hills. Statisticians routinely throw out the absurd values before computing the mean. Dorothy Denning pointed out the pun in their terminology (applicable to Byzantine agreement algorithms, where you don't trust anyone): the OUT-LIERS are really the OUT-LIARS.

EVEN WORSE, Jagan points out that if the clock had been accidentally set INTO THE FUTURE, things could also get very sticky. We also have a problem of nonunique clock readings during the hour at 2AM when Daylight Savings Time ends. A good time to be asleep. PGN]

[Here is some more background.]

Date: Mon 17 Mar 86 12:37:37-PST
From: Mark Lottor <MKL@SRI-NIC.ARPA>
Subject: [Louis A. Mamakos <louie@trantor.UMD.EDU>: time]
To: Jagan@SRI-CSL.ARPA

This was just to verify that the problem was on the remote system and not some local problem...

Date: Mon, 17 Mar 86 15:31:14 EST
From: Louis A. Mamakos <louie@trantor.UMD.EDU>
To: MKL@sri-nic.ARPA
In-Reply-To: Mark Lottor's message of Mon 17 Mar 86 11:34:41-PST
Subject: time

Yes, I can verify that it was indeed the clock (actually the host the clock was on) that was screwed up. It it unfortunate that there is no way to get the current year out of the WWVB clock. There was work being done in the computer room, which reset our LSI-11/73 host, which subsequently got confused. Sorry about the problem.

Louis A. Mamakos WA3YMH Internet: louie@TRANTOR.UMD.EDU
University of Maryland, Computer Science Center - Systems Programming

Clockenspiel

Jim Horning <horning@decwrl.DEC.COM>
17 Mar 1986 1436-PST (Monday)

Your errant clock reminds me of something that happened at Stanford in the mid-sixties. I was apparently one of the first users of the 360/67 to run a job that started on one day and finished on the next. When the statement for my account arrived in the mail, I had quite a job convincing my wife that the huge figure (to a graduate student couple) was nothing to worry about: It was a CREDIT resulting from a job that was charged for minus 23 hours and 58 minutes!

The Xerox Alto operating system had a compiled-in reasonableness check
on the date and time. When it started up, if the local clock wasn't
"reasonable," it sent a request over the Ethernet and put "Date and
Time Unknown" in the banner. Well, you guessed it: The day came when
the (correct) time from the time server was no longer "reasonable," and
therefore couldn't be corrected by appeal to the time server....

Jim H.

RISKS re: Cordless phones

<Chris.Koenigsberg@G.CS.CMU.EDU>
17 Mar 1986 11:48-EST

My roommate has a cordless phone and it goes on the blink every few weeks.
All the phones in the house stop working. When you pick any one up, all you
get is a very loud static sound and you can't dial out. I have learned that
I can fix this problem by sneaking in his room and unplugging the cradle for
his cordless phone. A visitor in the house was very frightened one night
when she was left alone and though someone had cut the phone lines or
something. It was the cordless phone on the blink again.

Chris Koenigsberg
ckk@g.cs.cmu.edu , or ckk%andrew@pt.cs.cmu.edu
{harvard,seismo,topaz,ucbvax}!g.cs.cmu.edu!ckk
(412)268-8526 office, (412)362-6422 home
Center for Design of Educational Computing
Carnegie-Mellon U.
Pgh, Pa. 15213

re: money talks

Dirk Grunwald <grunwald@b.CS.UIUC.EDU>
Mon, 17 Mar 86 16:44:15 CST

I read the 'money talks' article with great amusement. One of the risks to
society which is worth talking about is the risk of using inappropriate, or
downright silly, technology.

Talking money would appear to be such a waste of resources. Certainly some
other method of denomination descrimination could be devised for the
visually impared. Rasied lettering, coinage instead of paper money, different
sized paper money, different paper stock. But talking money?

dirk grunwald
university of illinois

Money Talks

<Matthew_Kruk%UBC.MAILNET@MIT-MULTICS.ARPA>
Mon, 17 Mar 86 09:07:32 PST

Correction to my previous message: The date of the article should be
March 14th (Friday).

[Non]computerized train wreck

<ihnp4!utzoo!lsuc!msb@seismo.CSS.GOV>
Mon, 17 Mar 86 19:04:03 EST

Me:
> Not only was this NOT a case of computer malfunction, but indeed, a more
> fully computerized system (with cab signalling and automatic train stopping)
> would probably have prevented the accident.

PGN:
> [... Thus, even though it appears NOT to be a computer problem,
> we discover that the computer could have done better! But, of course,
> don't blame the computer system. Blame the people who specified,
> designed, and implemented it -- not JUST the train operator(s). PGN]

You sound more critical than I meant to be. The cost of equipping all major railways with cab signalling and the like would be considerable, to say the least. While such installations certainly do exist, especially on busy high-speed lines, the "centralized traffic control" in use on the route in question is probably much more common. Are you calling on all railways to upgrade their signaling systems long before they are life-expired, every time something somewhat better comes along?

Mark Brader (ihnp4!utzoo!lsuc!msb and ...!dciem!msb are both me.)

[One would hope that new improvements do not always require everything to be thrown out. Long ago we discovered the advantages of software solutions over hardware solutions. But when human lives are at stake, safer systems may be worth the price of upgrading equipment. I think that the incredible escalation of law-suit awards and of rates for malpractice and liability insurance may provide some new incentives. PGN]

On-line Safety Database

"DYMOND, KEN" <dymond@nbs-vms.ARPA>
17 Mar 86 15:14:00 EST

Our Library Bulletin (and as a frequent user I'd have to say that the NBS has one of the best technical libraries going) for February contained a notice that Pergamon Infoline (evidently a supplier of such services) is offering a new online database service, SAFETY: "SAFETY, produced by Cambridge Scientific Abstracts, provides broad interdisciplinary coverage of safety, including industrial, transportation, environmental, and medical safety. This database indexes journals, books, reports, patents, and proceedings published in 1981 or later." If someone on the list uses this database, please let us know how well it covers computer and software safety.

Ken Dymond
National Bureau of Standards

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 2: Issue 30

Tuesday, 18 Mar 1986

Contents

Re: Classes of Errors

Scott Rose {206} 543-4226 <rose@uw-bluechip.arpa>
17 Mar 86 20:28:30 PST (Mon)

The dichotomy between errors of commission and of omission is reminiscent of the tension between negative and positive control in launch-on-warning systems. Clearly, negative control is a snap if one is willing to compromise positive control: there is perfectly reliable negative control whenever the system is shut off. That is, errors of omission are not possible if one is willing to accept errors of commission in this case. Obviously, there is a continuum of possibilities between this extreme and the extreme of just launching without any reliable detection whatsoever; this is the only region of interest. The point illustrated is that the two classes of error are not likely to be independently controllable; there is a built-in tension between them.

Range Safety System

David desJardins <desj@brahms.berkeley.edu>
Mon, 17 Mar 86 21:52:11 pst

I haven't seen anybody mention that there does seem to have been an "error of commission" in the operation of the range safety system after the Challenger explosion (specifically, the destruction of the SRBs). Of course this is a human rather than a computer error, but the result is the same; the system as a whole functioned less than optimally.

I understand that even NASA now admits that the SRBs were not in fact endangering anything at the time that they were destroyed. But I do understand how there must be an almost irresistible temptation for the range safety officer to do the "safe" thing (in this case, destroy the boosters). Perhaps this is the inevitable result of having humans making these decisions (error on the side of safety).

I'm not sure that anything can really be done about this, except to provide extensive training and an adequate supply of information on which to base the actual decisions. Do the range safety officers have access to real-time flight-path projections and similar information that would allow them to make intelligent decisions?

-- David desJardins

commission vs omission

<ST401385%BROWNVM.BITNET@WISCVM.WISC.EDU>
Tue, 18 Mar 86 11:06:01 EST

Martin J Moore queries why the shuttle destruct system should be tested more extensively against errors of commission (error causes destruct system to activate) than against errors of omission (error causes destruct system to be unable to activate). The reason is that for the errors of omission, the rest of the system serves as an additional link, ie., for an error of commission to cause disaster, ONLY the destruct system has to fail. For an error of omission to cause disaster, the destruct system has to fail SIMULTANEOUSLY with the vehicle failing. Thus, the most probable event is for an error of omission to gail "safe": the vehicle wouldn't have blown up if somebody wanted it to, but nobody wanted it to, so it didn't matter.

--Geoffrey A. Landis, Brown University
Reply to: ST401385%BROWNVM.BITNET@WISCVM.ARPA

Stupid Clock Software

Dave Curry <davy@ee.purdue.edu>
Tue, 18 Mar 86 08:39:44 EST

Here at Purdue's Engineeering Computer Network, we've had "synchronized" time on all our machines for some time. For a long time, all the machines ran "datesync", a program which checked a central machine every N minutes (usually 15 or 30) and set the local machine's date and time according to what it got from the central host. There were some minor sanity checks, but nothing fancy. We never had too much trouble, since if the central machine came up with the wrong date you could get it reset before the other machines came and got their time information.

A couple of years ago, we plugged a Heathkit (Al)Most Accurate Clock (WWV) into the central machine. It used to be set off "George's Watch". This made stuff somewhat better -- when the central machine came up, it got the time from WWV instead of "datesync"ing to another machine. The WWV software was used periodically (every 15 minutes, I think) to adjust the central machine clock. Except for the time when the someone unplugged the WWV clock and then a few days later it's battery backup freaked out, we have NEVER had a serious problem with the "datesync" scheme (20 machines or so).

Well, with 4.3BSD UNIX you get this neat toy called the "time daemon". It handles network clock synchronization off a master machine by doing various clock adjustments (rather than hard-setting the clock, it actually diddles the clock speed). It has all these neato sanity checks and SUPPOSEDLY it won't let a preposterous time come in. In fact, you even see this stuff on the console once in awhile that says "PREPOSTEROUS TIME ....". Sounds neat, right?

Well, last month all the machines on the network decided that it was 4:00pm, January 4, 1985. Somehow this slipped right by all the sanity checks, and the master time daemon stuffed it into one machine. Then it PROPAGATED it to all the other machines. Having horribly wrong time can be fairly catastrophic on a UNIX system -- the "cron" utility starts up all sorts of programs based on the time of day and day of the week. Including things like "find all files older than X and delete them". We were less than amused... Another brain-damaged feature of the time daemon -- if you set the date on ONE machine, it BROADCASTS that information through the time daemons to ALL the machines. You better PRAY you never mistype the date!

The thing that really bugs me about this stuff is that it's so simple to make it more bullet-proof (not fool-proof, necessarily). For example, just plain IGNORE any date which changes your date by more than X unless you are explicitly told TAKE THIS DATE REGARDLESS.

Well, this letter is already twice as long as I intended, so I'll shut up now... things like this are an interesting subject though -- I wonder how much other software in computerdom just blindly assumes that some "authority" is correct.

--Dave Curry
Purdue University

Control characters in headers from eglin-vax

"MARTIN J. MOORE" <mooremj@eglin-vax>
0 0 00:00:00 CDT

In addition to its other bugs (e.g., null timestamps), our mailer puts a control character at the beginning of each user's personal name. This arises from keeping the personal name as a counted string but displaying it as ordinary text; the control character is the count byte. Recently I have received messages (ranging from polite to nasty) from several RISKS readers telling me that my control character causes their terminals to reset, go into graphics mode, or do other unpleasant things. I can't do anything about it; we're waiting for a fix from the vendor, and we're stuck until we get it. Since you edit my headers to get the date right, would you mind flushing the control character also?

mjm

[I took it out of the FROM field. But this problem reminds me that many of our readers may not have never heard of the old problem of squirreling away control characters and escape sequences in messages which when read can wreak havoc with an unsuspecting mail reader, especially one with an intelligent terminal having redefinable keys. If that problem has not been fixed on YOUR system, dear reader, YOU may be running at great risk. PGN]

Money Talks

Prasanna G. Mulgaonkar <PRASANNA@SRI-AI.ARPA>
Tue 18 Mar 86 09:05:17-PST

One of the origin of risks in any system is exemplified by the discussion of the Canadian effort at "vocalizing" the value of a currency note. I do not have any information in addition to what has been posted in the RISKS digest (so feel free to correct me if I am wrong), but there seems to be nothing in the original posting [RISKS 2-28] to indicate that the aim of the device is to dectect/reduce forgeries. Yet, the first argument offered against it is the ability to fool it.

My interpretation of the device is one to help a blind person "read" the currency note SOMETHING THAT HE CANNOT NOW DO--- not to tell him if the currency note is valid or a forgery! Risks of such a system come from the public putting more faith or expecting more from a system than its stated goal.

As a side issue, there is no reason to think that fooling such a device would be any different than fooling change machines that are commonly found around here, which detect at least the difference between 1$ and 5$ bills. There is no reason why such a machine could not be connected to a voice synthesizer to speak out the amount. Addition of speech capability in itself does not increase the risks/unreliability/foolability(?) of any system.

--Prasanna

[Just don't trust it with anything larger than what you are willing to be cheated out of. You may have noticed that you don't see change machines for $100 bills. There are good reasons. PGN]

Search RISKS using swish-e

Report problems with the web pages to the maintainer

Search RISKS using swish-e

THE RISKS DIGEST

Forum on Risks to the Public in Computers and Related Systems

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

Volume 2: Issue 31

Wednesday, 19 Mar 1986

Contents

Still more on shuttle destruct systems

"MARTIN J. MOORE" <mooremj@eglin-vax>
0 0 00:00:00 CDT

>From: desj@brahms.berkeley.edu (David desJardins)
>[T]he destruction of the SRBs...is a human rather than a computer error.

It was certainly a human action but I do not agree that it was an error.
That we now -- long after the fact -- would like to retrieve the boosters
is unfortunate; but had they not been destroyed they would either have
ended up in the drink anyway (possibly much further away from the Cape and in
much deeper water, making the recovery even more difficult than it is) or they
would have endangered a land area.

> NASA admits that the SRBs were not in fact endangering anything at the time
> that they were destroyed...there must be an almost irresistible temptation
> for the range safety officer to do the "safe" thing.

First, the destruct decision does not come from NASA; it comes from the Air Force. Second, there is no "temptation" involved; the range safety officer MUST DO the safe thing based on the information available in real time. He did so. For more on the information available to the RSO, see below.

> Perhaps this is the inevitable result of having humans making
> these decisions (error on the side of safety).

Would you prefer error on the side of non-safety? Or are you advocating the use of computers to make the actual destruct decision? If the latter, you will have a hard time getting anyone to fly the vehicle! Also, in the Challenger case, a computer would have made the same decision to destroy the SRBs. While I was at the Cape, there was some investigation into the possibility of automating the destruct decision; it was decided that even if it were safe and reliable, it could only be used on unmanned launches. Since the number of unmanned launches would decrease dramatically in the coming years, an automatic destruct decision system would not be cost-effective.

> I'm not sure that anything can really be done about this, except to
> provide extensive training and an adequate supply of information on which
> to base the actual decisions. Do the range safety officers have access
> to real-time flight-path projections and similar information that would
> allow them to make intelligent decisions?

The RSO's do receive *extensive* training. Being an RSO is a full-time job, not an extra duty; the RSO's are either Air Force officers or high-grade civil servants (incidentally, I was once encouraged by some of the RSO's to apply for an opening in their number. I am REALLY glad I decided not to!). Their training includes realistic launch simulations in which various things go wrong. The problems include not only wild trajectories but equipment and people problems; during the simulations, one of the RSOs is in charge of setting up the problems. They perform this duty on a rotating basis and it is quite competitive. In addition to the real-time training, there is "office" training in which they study the effects of various missiles, possible debris footprints, etc.

Regarding flight projections: tracking data are gathered from a variety of sources, including radars, inertial guidance telemetry, and optical trackers (mainly used very early in flight when radars are ineffective due to multipath.) The tracking data is fed to the Central Computer (redundant Cyber 740s) where through various filtering and checking the two "best" sources are chosen, and used to determine the vehicle's position and velocity, and to compute from them the Instantaneous Impact Point (IIP), which is the point at which the vehicle would impact if thrust were to terminate at that instant. The RSO has a lot of information displayed on his consoles: the primary and alternate position, velocity, and IIP, real-time telemetry from the vehicle (e.g., engine chamber pressures), live video coverage, and others. The RSO uses this information (plus comm links to the Flight Director in Houston on a manned launch) to make his decisions. The present position itself is not critical; it is the IIP that determines when an area is endangered. The RSO has displays of the nearby land masses, with "destruct lines" drawn some distance out to sea; if an IIP crosses a destruct line, the land area is endangered and the missile should be destroyed. Also, if a vehicle is obviously wild (such as an orphaned SRB) it should be destroyed while still in a safe area *before* it can endanger the land mass! This is why the RSO's decision was not an error. As I understand it, although the SRB had not yet crossed the destruct line, it had curved back toward the coast and would have crossed the line in a few seconds.

From my observations, I evolved my own rough rules-of-thumb for destroying a missile. These are purely my personal observations, they're not official, and they're pretty general, so please don't nitpick at them.

```
----
IF (missile is unmanned) THEN
   IF (IIP crosses destruct line) OR (missile is obviously out of control)
   OR (missile is out of communications for a length of time sufficient
   to endanger any area from its last known position) OR (pad disaster occurs
   -- e.g., vehicle falls over after ignition) THEN
      Destroy the missile.
ELSE IF (missile is manned) THEN
   IF ((IIP crosses destruct line) AND (Houston reports the flight crew is
   *not* in control of the vehicle)) OR (pad disaster occurs) THEN
      Destroy the missile.
END IF
----
```

SRBs flying by themselves are certainly unmanned and obviously out of control.

Sorry about the length of this message, but I'm getting a little tired of hearing people second-guess the RSO's decision. The RSO in question is one of the most intelligent and capable individuals I have ever known; he made the correct decision based on the real-time information, and that's what he is supposed to do. One SRB was heading toward the coast, and even though it had not yet crossed the destruct line, the risk to the population was significant (and increasing). He unquestionably made the right decision based on the information at the time.

Martin Moore

Disclaimer: I disclaim everything.

Clock Synchronization

<Andy_Mondore%RPI-MTS.Mailnet@MIT-MULTICS.ARPA>
Wed, 19 Mar 86 09:38:18 EST

The recent discussion of computer clocks showing the wrong time has reminded me of a related problem -- clock synchronization on computers. For example, I will sometimes receive a message from someone on another host on campus where the "time received" on my host will be earlier than the "time sent" on his machine! Granted, clock synchronization with electronic mail isn't really that critical, but I can think of a lot of other applications where having clocks out of sync with each other would be totally unacceptable.

Timestamp integrity at system startup

John Coughlin <John_Coughlin%CARLETON.BITNET@WISCVM.WISC.EDU>
19 Mar 86 10:56:56 EST

The CP-6 operating system has an interesting integrity check for timestamp setting. On a warm or cold boot the operator is asked for the date and time. This is compared with the timestamp on the last error log entry. If the 'new' timestamp is earlier than the error log entry or is more than nine hours later then a timewarp error is reported and confirmation is requested. If the operator chooses to reject the time he entered he can make a correction.

There are two problems with this system. First, if a new system is being built there are no error log files. I think the base time stamp (1978-01-01 00:00) is used in this case. Second, it is possible for there to have been no error recorded in a nine hour period. This actually happened to us a couple of times, so we now write a dummy error log entry every four hours. I am thinking of stepping this up to once per hour in case the system is down at exactly 00:00 or 04:00 or ...

This system has its drawbacks, but helps to reduce the risks of setting an unreasonable timestamp at system startup.

/jc

Danny Cohen on SDI

<crummer@aero>
07 Mar 86 20:23:58 PST (Fri)

[SINCE MY GUESS IS THAT MOST OF YOU ARE NOT READING SOFT-ENG@XX.LCS.MIT.EDU, IT SEEMED WORTH INCLUDING THIS HERE. PGN]

The following is a "summary" of a talk given by Danny Cohen of ISI. Dr. Cohen is chair of the SDI Organization (SDIO) and a member of the "Eastport Group", a panel on computing in support of battle management:

The Eastport Group panel was appointed to devise an appropriate computational/communication response to the SDI battle management computing problem and make recommendations for a research and technology development program to implement the response.

The panel concluded that computing resources and battle management software for a strategic defense system are within the capabilities of the hardware and software technologies that could be developed within the next several years.

However, the anticipated complexity of the battle management software and the necessity to test, simulate, modify, and evolve the system make battle management and command, control, and communication (BM/C3) the paramount strategic defense problem.

Software technology is developing against inflexible limits in the complexity and reliability that can be achieved. The tradeoffs necessary to make the software task tractable are in the system architecture. The "applique approach" of designing the system first and then writing the software to control it is the wrong approach is the wrong approach for SDI. System architecture and battle management must be developed together. This was suggested in an earlier report on SDI known as teh Fletcher Report.

One promising class of system architectures for a strategic defense system are those that are less dependent on tight coordination that what is implied by the Fletcher Report. The advantages of this type of architecture include robustness, simplicity, and the ability to infer the performance of full-scale deployment by evaluating the performance of small parts of the system.

The panel prefers an unconventional architecture that simplifies the software development and testing tasks over reliance on radical software development approaches and the risk that reliable software could not be developed by the "applique approach" at any cost.

Two more mailer problems

"Sidney Markowitz" <SIDNEY%OZ.AI.MIT.EDU@XX.LCS.MIT.EDU>
Wed 19 Mar 86 16:34:28-EST

1) I did not personally see this, but I was told that Symbolics briefly introduced a new feature in their mail program with the current release of the operating system. It was a new header line that a sender could use to include graphics as part of the mail message. This was implemented by having the header line include a lisp expression that would be evaluated (executed) when the receiving mailer loaded the message for display. Somebody pointed out the other possible ways in which an arbitrary piece of executed code in a mail message could be used, and that feature was dropped very quickly.

2) This is not quite on the same level as the above problem, or the old control character in the message trick, but the following message appeared in my mailbox some 5 or 6 times over the course of a couple of days. It's relevant to RISKS as yet another real life example of "nothing can go wrong... go wrong... go wrong..."

The message was sent to a net distribution list:

[begin edited forwarded message:]

To: info-gnu@PREP.AI.MIT.EDU, info-gnu-emacs@PREP.AI.MIT.EDU
Subject: Duplicate messages

1) Apologies from the chief gnu list maintainer.

2) For a variety of reasons, this happens intermittently on prep, an

MIT AI Lab machine the lists are hosted on. For a variety of reasons, there is little that the GNU staff can do about it, at this time.

3) Thanx for your patience.

[End of edited forwarded message]

Sidney Markowitz <sidney%oz@mit-mc.arpa>

bounced mail - i bet that this is for y'all? [THANKS]

Andrew Scott Beals <bandy@lll-crg.ARPA>
Wed, 19 Mar 86 14:46:25 pst

From ucdavis!uucp Tue Mar 18 22:41:20 1986
Date: Tue, 18 Mar 86 22:17:29 pst

Mail failed. Letter returned to sender.
>From seismo!harvard!think!mit-eddie!genrad!panda!talcott!maynard!campbell
  Tue Mar 18 21:30:28 1986 remote from lll-crg
          [...AS USUAL, I DELETED THE ROUTING, ALTHOUGH IT WAS EXCITING...]
Date: Tue, 18 Mar 86 17:36:01 EST
To: ucdavis!ucbvax!sri-csl.arpa!
Subject: Why would anyone want to computerize voting?

Why would anyone want to computerize voting? Doing so only increases the risk of fraud, by reducing the number of people involved in the process. ("The best deterrent to crime -- witnesses.") Elections don't happen often enough that saving money can count for much -- in fact, I believe around here ballot counters are unpaid volunteers. Rapidity of the count? Who cares whether the results are known in two hours or two days?

Sounds like yet another scheme (remember "computer literacy"?) to enrich computer companies at the public's expense.

[There are of course lots of reasons for automating. But PLEASE, let's not get a flurry of messages answering that one here. This is just another fine example of a more complicated solution introducing new vulnerabilities and different risks. PGN]

Larry Campbell   The Boston Software Works, Inc.
ARPA: maynard.UUCP:campbell@harvard.ARPA   120 Fulton Street
UUCP: {harvard,cbosgd}!wjh12!maynard!campbell Boston MA 02109

Marking money for the blind

Atrocity Joelll <Joelll%UMass.BITNET@WISCVM.WISC.EDU>
Wed, 19 Mar 86 18:02:22 EST

On the subject of the bill-denomination-determining in Canada, there is a method that I noticed is in use in Israel when I was there recently: on every denomination of shekel notes there is a unique raised pattern of lines for the use of the sight-impaired and to aid in annoying counterfeiters. For example, on the five-shekel note there are three dots formed of these lines, each about 4 mm in diameter, and on the 500 shekel note there is an oval shape made of the raised lines about 12 mm long and 4 mm wide.

The biggest benefits of this system, in addition to making counterfeiting harder, are that is is cheap, there is no computer 'denomination reader' to have vandalized, and that the blind persons who use this service wouldn't have to go out and find one of these silly machines...

Atrocity Joelll
JOELLL%Umass.Bitnet@wiscvm.wisc.edu

[One must carefully examine the code of raised symbols to see how easily a lower denomination can be changed into a higher denomination. In Braille, for example, it is easy to change a TWO into a ONE (assuming the fingers do not detect a rough flattened spot) and a ONE into a TWO (by raising an extra spot). By the way, there are situations in which one might wish to make a higher denomination appear as a lower denomination... fooling a blind customs official with Altered Braille? 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 2: Issue 32

Thursday, 20 Mar 1986

Contents

Om/Comm-ission, and analysis of risks

Niall Mansfield <MANSFIELD%DHDEMBL5.BITNET@WISCVM.WISC.EDU>
Thu, 20 Mar 86 12:30:42 n

It is often difficult to decide whether an action carried out really is a fault of omission or commission. As is so often said, many program failures are due to not considering a possible set of circumstances, which when it occurs causes the program to act improperly. In such cases, the damage is certainly an act of commission, but the real failure is the omission to predict the failure. I think that any attempt to distinguish formally between om/comm-ission is likely to lead to sophistic arguments distracting attention from the real cause of the problem.

Another unproductive approach seems to be suggested by something PGN said in RISKS-2.27:

> A fine example of the risks having to include people, not just
> computers, and of a more pervasive role of the computer than meets

> the eye -- indeed a more human-oriented computer system might have
> helped! Thus, even though it appears NOT to be a computer problem,
> we discover that the computer could have done better!

There are very few cases where a system which has failed could NOT have done better, so saying it doesn't advance our understanding. It seems that because RISKS is about computer risks, then we will do our best to find a computer cause for every failure. (Remember the immediate speculation after the Shuttle disaster about how a computer could be shown to be responsible).

Surely RISKS should concentrate on failures that occur because of computer involvement but which would not have occurred with a human-only system, because systems are always going to fail. As Murray.pa@xerox pointed out in RISKS-2.21, there are risks involved in not using computers, where such use can lead to saving lives: if a system is doing superb work 99% of the time, it is fruitless to pick on the 1% failure, and jump on the bandwagon saying "Ohhhhhh, the computer's run amok, isn't it terrible". We must keep risks and benefits in perspective. As PGN finished off:

> But, of course, don't blame the computer system.
> Blame the people who specified, designed, and
> implemented it -- not JUST the train operator(s).

This is the heart of the matter - we are looking at the risks (presumably) so that we humans, the makers of systems, can avoid the same mistakes, not just for the malicious pleasure of beating the drum about somebody else's shortcoming.

(So maybe I don't disagree with PGN after all).

RSO's and IIP's

Dave Curry <davy@ee.purdue.edu>
Thu, 20 Mar 86 07:44:56 EST

One thing keeps nagging at me after reading your explanation of RSOs and IIPs. I suspect it's more from my lack of knowledge about trajectories and launching things and such than anything else. Anyway, here goes...

You said several times that if the IIP ever crosses the "safety lines" then the missile should be destroyed. What I'm confused about is this: does this mean that under "normal" circumstances the IIP never crosses these lines, or do you mean the missile should be destroyed only if something is "wrong"? It seems to me (again I know very little about launching things and such) that if the IIP can never go "that way" then you are limited in the directions you can send a rocket (come to think of it I guess I've never heard of a launch going "back" over the U.S. to get somewhere...).

Also, where does the consideration of the IIP stop? Something sticks in the back of my mind that the shuttle flies over land masses (isn't there someplace in Rota, Spain where they can abort?). If it does, does this mean the IIP itself never touches the land masses, or does the IIP become less important after the missile reaches a certain speed/altitude/trajectory?

Thanks,
--Dave Curry

Complex systems ru(i|n)ning our cities

Mike Mc Namara at ESL Sunnyvale Ca <lll-lcc!tflop!mac@lll-crg.ARPA>
Wed, 19 Mar 86 19:07:42 pst

In pursuit of new directions for the RISKS forum, and in response to a recent article in the New Yorker Magazine, I bring up the subject of the risks inherent in the complex systems in which we live. We've probably all heard talk about how few hours New York City could survive without power/ water/subway/ etc, but perhaps it is worth discussing in this forum.

The article in the NYM is written from the perspective of a resident of a self-sufficient rent controlled apartment in the Village, who feeling quite smug about his castle, suddenly notices all the holes in the wall. There is the hole letting in electricity, the one for natural gas; there are lines for taking out the sewage, and lines bringing in fresh water.

This writer wonders where these lines lead. He then takes us along in his search to James Bay in Canada, where New York gets some of its electricity from hydroelectric plants. He takes us to Arizona, where some of the uranium for the Indian Point reactors is mined. He takes us to Brazil, where Con Ed gets the low quality diesel oil to burn to make electricity.

Similarily, he takes us upstate to the many reservoirs which supply New York with its world famous water. He follows the gas mains to Louisiana.

And so on.

I offer to the risk readers the question, How intelligently are we managing the risks assumed by the creation of our complex cities? We build systems so that millions of people can live in areas that are really deserts. What risks exists because of the creation of a L. A. that relies on 500 mile aqueducts to supply life-critical water? Who is in charge of insuring adequate safe guards? Budget conscious, 2 year term politicians, or life time members of water boards? The ramifications of any single failure of a utility system can probably be maintained via such a board that takes the long view and has the capitol to implement long term strategies.

But what about the interdependencies of utilities? What would a water shortage do to a nuclear power plant, that perhaps required cooling water that simply wasn't available? What would a collapse of the telephone system do to a natural gas distribution system that used remote pressure regulators that were controlled via telephone links?

What organizations exist to worry about such things, so I rest assured that there is no problem, and get some sleep at night?

What inter-system crashes are the readers aware of, that they might
share with this list?

Re: Two more mailer problems

Bernard S. Greenberg <BSG@SCRC-STONY-BROOK.ARPA>
Thu, 20 Mar 86 11:15 EST

> Date: Wed 19 Mar 86 17:54:33-PST
> From: RISKS FORUM (Peter G. Neumann, Coordinator) <RISKS@SRI-CSL.ARPA>
>
> Date: Wed 19 Mar 86 16:34:28-EST
> From: "Sidney Markowitz" <SIDNEY%OZ.AI.MIT.EDU@XX.LCS.MIT.EDU>
> Subject: Two more mailer problems
> To: risks@SRI-CSL.ARPA
>
> 1) I did not personally see this, but I was told that Symbolics briefly introduced a new feature in their mail program with the current release of the operating system. It was a new header line that a sender could use to include graphics as part of the mail message. This was implemented by having the header line include a lisp expression that would be evaluated (executed) when the receiving mailer loaded the message for display. Somebody pointed out the other possible ways in which an arbitrary piece of executed code in a mail message could be used, and that feature was dropped very quickly.

This is utterly and wholly false. No one here would be so naive.

Bernard S. Greenberg, Symbolics, Inc., Cambridge, Mass.

Banknotes for the visually handicapped (RISKS-2.31)

<roberts%forty2.DEC@decwrl.DEC.COM>
Thursday, 20 Mar 1986 01:59:05-PST

The Netherlands uses a similar system of raised impressions. High denominations are distinguished by different symbols (e.g. the H.Fl 50 note has a raised triangle, while lower notes such as the 10 and 25 have dots). I'm afraid I don't know what the new H.Fl 1000 notes have --- I don't see them very often :-). Britain, on the other hand simply uses different sizes of paper for different denominations, as does West Germany.

Nigel Roberts, Reading, England
[Different sizes of paper don't help the visually handicapped discriminate copy-machine products from originals.... PGN]

Banknotes for the visually handicapped

Barbara E. Rice <rice@nrl-csr>
Thu, 20 Mar 86 10:51:27 est

With all the talk about fooling the visually impaired by altering raised marks on bills or the magnetic ink, has anyone considered how small a population they are dealing with? My uncorected vision went beyond legally blind twenty years ago and has continued to go down hill since then. Without my glasses I can not see the eyechart much less any letters on it (with my glasses I can just scrape by a driver's eye exam). So I conducted a test here with my glasses off I was able to distinguish between a five and a one dollar bill at 6 feet (much further than arm's length).

So the population that could be fooled by such means I would say is relativlysmall, too small to it be worth anyones time and effort to steal from them. It would also be risky. Most people remember where it is that they get money from and where they have bought things. Anything larger than a $20 I definitely know where I got it. The error would be picked up by any sighted person dealing with the blind person not just an expert in conterfeit detection thus the altered bill would be rapidly discovered. So a person using this scheme would have to be constantly on the move and not collecting very much for his efforts. For most large puchases people use creditcards or cashiers check. Purse snatching or mugging would yield a better risk and effort vs profit ratio.

The point I hope I made is that thinking of methods to get around marking intended to help the blind is an interesting mental excercise but none of the methods thought up is a reason for not putting aids to the blind on currency. (really a blind customs agent? How many are there and how would you guarentee you got him? With my luck he would call in sick that morning and then I would really be in trouble.) A better reason for not using such aids is the small number of people who would benefit by it, but then you should consider the number of would be conterfeiters it might frustrate into trying other means of getting rich quick. That would be a good systems trade off problem.

[Come on, now. You think the example of the blind customs agent was serious? I was trying to give you an example where reducing the value consituted a risk. The problem is one of vulnerabilities. Pacemakers and automobile microprocessors are fine. But there are some very serious risks that must not remain unconsidered. Of course there are advantages to currency interpreters. But are they designed so poorly that they accept blank pieces of paper with funny symbols embossed on them? Do they introduce new risks that never existed before? PGN]

Psychological and sociological consequences

<ERA01%DHAFEU11.BITNET@WISCVM.WISC.EDU>
Thu, 20 Mar 86 11:27:54 cet

We are preparing a study about the psychological and sociological consequences if young people have intensive contacts with (home-) computers. So, we are looking for empirical studies (in wide spread) dealing with that subject.

Especially we are searching for articles about
- different methodological approaches (e.g. analytical, ethnological, qualitative and quantitative aspects ...)
- empirical designs and ideas
- results.

If you have any information (or know anyone who has) please help us.

Contact HARALD BAERENREITER, Fernuniversitaet, Arbeitsbereich Allgemeine
Soziologie, Postfach 940, D-5800 Hagen, F.R.G., or NETMAIL to FROM: field.
Thank you for being so helpful.   Harald.

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 2: Issue 33

Sunday, 23 Mar 1986

Contents

RSO's and IIP's - Martin Moore's response

Dave Curry <davy@ee.purdue.edu>
Fri, 21 Mar 86 08:00:21 EST

This is Martin Moore's response to my questions about RSO's and IIP's which appeared in RISKS-2.32. It is forwarded with his permission. Dave

------- Forwarded Message

Good question...I guess I forget that not all of the audience is familiar with space launch details and orbital mechanics. I'll try to explain the IIP's relation to the world and how it is used...

Simply stated, the IIP of an object is the intersection of its ballistic trajectory (or "orbit") with the surface of the Earth. An object is in a ballistic trajectory when it is not accelerating under its own power; its acceleration is due only to gravitational effects (in short, it's falling.) The trajectory can be determined almost entirely from the object's position (mostly altitude) and velocity vector relative to the Earth (there are minor effects due to aerodynmaics and various anomalies but these can be ignored for this type of calculation -- they take a great deal of computation to yield a relatively small correction.) An object which is resting on the Earth's surface is located at its IIP. An object in free orbit does not have an IIP;

its orbit does not intersect the Earth's surface. For an object falling through the atmosphere (which is what our missile would do if its thrust terminated) the IIP becomes interesting.

Since the IIP is the end result of an object's ballistic trajectory, the IIP does not change when the object is not accelerating; conversely, while the missile is accelerating, the IIP moves downrange *FAST*. (Consider that the Challenger explosion occurred 8 miles or so downrange, but most of the pieces impacted 20-40 miles downrange.) So on a normal missile launch the IIP starts on the launch pad; as the missile launches the IIP moves downrange very fast until it eventually moves off the planet (if an orbital launch) or to the target area (for a weapons test) or something is wrong. On a shuttle launch, the IIP has moved off the planet by MECO (about +520 seconds); the shuttle's engines cut off even though it has not yet achieved orbit -- it "coasts" on up to orbit based on the velocity vector it has achieved through powered flight.

Now, to answer your question, missiles launched at the Cape NEVER fly over land intentionally except at the very first seconds (unavoidable) or during a shuttle landing (when the Orbiter is flying by itself and the dangerous parts have been dropped.) This is why the launch facility at Vandenberg was built; shuttles cannot be launched into polar orbits from the Cape because there is land both due north and due south. On *any* launch, violation of the destruct lines means something is wrong (they are drawn with the missile's nominal trajectory in mind) and the population is endangered. Missiles can be obviously bad *without* crossing the destruct line; if a second stage, say, fails to ignite, the IIP stops halfway downrange and the missile falls into the drink. It is generally wise to blow it up in this case as if it falls intact the fuel is not very good for the environment. Unmanned missiles are pretty easy: something goes wrong, you blow it up. Obviously, this has to modified with the Shuttle; if it's performing an abort you don't blow it up (the tanks and solids are already gone; the Orbiter is no threat.) If it goes awry and curves back over land *but* the crew is still in control (which is at least theoretically possible) you let it go as long as they are in control -- they may be able to recover for a landing or at least get it back over the ocean, drop the tank (you don't want to blow it over land -- would shatter every window in Brevard County), and try to ditch and have at least a chance of surviving.

Whew. I hope this has answered your question. Feel free to follow up if it hasn't or if you have other questions.

/mjm

- ------

------- End of Forwarded Message

Omissions/commissions and missile destructs

Chris McDonald SD <cmcdonal@wsmr06.arpa>
Fri, 21 Mar 86 13:09:06 MST

Regarding Dave Curry's musings about his never having heard about a "missile going back over the US", in fact missiles go over the US on a daily basis at White Sands Missile Range. As a 4,000 square mile DoD test facility the Range has been an inland range for missile and rocket firings for over 40 years. This fact has some bearing on the discussion of omissions/commissions in flight safety computers because major cities surround the Range resulting in legitimate safety concerns. During the last 40 years not every flight has range boundaries and in one well-publicized incident a rocket landed in a Juarez, Mexico cemetery. While redundancy in flights safety computers has so far precluded an accident or incident attributable to a computer, there was one incident in which a missile was destroyed by computer because of a breakdown in trajectory tracking data transmissions. The computer was programmed to automatically destroy the missile if it did not have tracking data from a specified number of radars. The rationale behind this was that, if one lost radar track given the manner in which the test was structured, the missile was well off course and should be destroyed. Even though there was redundancy in radars, a situation occurred in which radar problems precluded the flight safety computer from receiving the anticipated tracking data. Launch occurred and from all personnel accounts appeared to be nominal. But in fact the computer was not receiving the tracking data immediately after launch to predict what another contributor referred to as IIP or Instantaneous Impact [that] destroyed the missile. All readers can well understand that the project manager for the missile system involved was extremely upset over the destruction of his test item.

Blind and Paper Money

<celerity!sdo@sdcsvax.ucsd.edu>
Sat, 22 Mar 86 14:35:40 pst

One solution I have heard proposed to the problem of the blind being unable to read the denomination of paper currency is to cut off the corners of the bills.

```
   The $1   bill would have 4 corners cut off.
   The $5   bill would have 3 corners cut off.
   The $10  bill would have 2 corners cut off.
   The $20  bill would have 1 corners cut off.
   The $100 bill would have 0 corners cut off.
```

Forgery would be limited since cutting of a corner of a bill would decrease its value.

This is much simpler and less costly than "talking money".

> [This may seem unrelated to Computer RISKS. However, in some cases -- believe it or not -- the best solution may not involve technology. However, this solution still begs fraud by copy machine. It is easy to cut corners off of a copy... But, let's blow the whistle on this topic for now. PGN]

It would take someone really sophisticated, with a Ph.D in math or CS.

22 Mar 1986 12:50-PST

This story made the front page of the Palo Alto TimesTribune:

a775 21-Mar-86 12:32 ny BCBURGLARY
Two Cases of Computer Burglary
(WashPage) c.1986 N.Y. Times News Service

WASHINGTON - Jennifer Kuiper was working late at her computer terminal in the office of Rep. Ed Zschau of California on March 7 when she heard a beep that told her someone had entered the computer system from an outside telephone line.

Twenty minutes later, her computer screen went blank. When service was restored, copies of more than 200 letters sent to constituents and iformation on mailing addresses had disappeared.

Four days later, staff workers for Rep. John McCain of Arizona told the police they had discovered that someone outside their office had reached into McCain's computer and destroyed hundreds of letters and mailing addresses over the lunch hour.

Why the computers were entered from the outside, and by whom, is now the subject of a criminal investigation by the Capitol police and the United States attorney for the District of Columbia. They say the have ruled out the possibility of staff error in destruction of the records and have some leads. But they refuse to discuss possible motives.

Both Zschau and McCain are Republicans, neither yet a House leader but both increasingly visible on Capitol Hill. Both are seeking Senate seats in the November elections.

These were apparently the first computer break-ins on Capitol Hill, where computers are increasingly being used, especially for recordkeeping and answering mail.

''This is definitely a concern,'' said Inspector Robert R. Howe of the Capitol police. ''We're looking into better controls to prevent it from ever happening in the future.''

Zschau, who taught computer courses at Stanford Business School, and founded and for 13 years was president of System Industries, a computer software company, said the illegal entering of his office computer was ''tantamount to someone breaking into my office, taking my files and burning them.''

''I am very concerned,'' he added, ''and the police would be more concerned if this were a physical break-in.

''Because people don't see the files overturned or a pile of ashes outside the door, it doesn't seem as bad,'' he continued. ''But it is equally as devastating. We rely on computers a lot for correspondence, writing articles and keeping a record of the history of the letters and responses sent to our constituents.

''Every office on Capitol Hill can be broken into in this way and the files deleted. It can bring the work that a member of Congress does to a complete halt.''

After both break-ins, the copies of most of the lost records were regained from duplicate files. ''We were lucky,'' said James M. LeMunyon, administrative aide to Zschau. ''We had back-up computer tapes that restored all but 30 of the 200 letters. My greatest concern was that they might have destroyed our lists of constituents' names.''

Stephen A. Armstrong, vice president of Micro Research, the company that provides computers and related equipment to more than 150 members of Congress, including both Zschau and McCain, said that whoever broke into the computers ''would have to have a password and two security codes to get in.''

In a congressional office that has computers, the system operates independently of systems in other offices, and each staff member has a personal password to gain access to computer files.

For someone to enter the system by telephone from outside the office, a special switch in the office must be on.

''It is possible to break into a system if all physical and software security measures are ignored,'' Armstrong said.

''But it would take someone really sophisticated, with a Ph.D. in math or computer science.''

nyt-03-21-86 1532est

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 2: Issue 34

Thursday, 27 Mar 1986

Contents

Re: RSO's and IIP's - Martin Moore's response

<ihnp4!utzoo!henry@seismo.CSS.GOV>
Wed, 26 Mar 86 20:45:04 EST

> Now, to answer your question, missiles launched at the Cape NEVER fly over
> land intentionally except at the very first seconds (unavoidable) or during a
> shuttle landing... This is why the launch facility at Vandenberg was built;
> shuttles cannot be launched into polar orbits from the Cape because there is
> land both due north and due south...

As an example of how bureaucratic priorities can sometimes override known safety considerations, it is worth noting that the Office of Mismanagement and Bean-counting did suggest saving the cost of the Vandenberg shuttle facility by launching north from KSC. This idea was a non-starter for about five different reasons, range safety not least. It's amazing that it was ever suggested, but it was -- quite seriously.

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

Range Safety: a final word

"MARTIN J. MOORE" <mooremj@eglin-vax>
0 0 00:00:00 CDT

Apparently I confused a few people judging by the mail I've gotten...what I said about missiles launched at the Cape not flying over land applies ONLY TO MISSILES IN THE LAUNCH PHASE. Obviously, satellites in orbit pass over a large part of the Earth's surface. And as another contributor pointed out, some test ranges routinely fly missiles over land; I was talking only about the Cape, which does not.

I think this discussion is reaching the point of diminishing returns from the RISKS viewpoint. I will continue to answer detailed questions by personal mail, but let's move them out of RISKS.

/mjm [PGN concurs.]

Someone really sophisticated, with a Ph.D...

<roberts%forty2.DEC@decwrl.DEC.COM>
Monday, 24 Mar 1986 05:26:49-PST

----------reply to mail dated 24-MAR-1986 06:19 [RISKS-2.33]-----------

> ''It is possible to break into a system if all physical and software
> security measures are ignored,'' Armstrong said.
> ''But it would take someone really sophisticated, with a Ph.D. in math
> or computer science.''

Since when does a Ph.D in math, or even one in Computer Science, teach you how to be a hacker (either kind)?

Most of the "Computer Burglars" I have come across were entirely self-taught.

Nigel.
[I presume that is why Geoff titled it the way he did. It is guys such as Armstrong who are headstrong -- except that their heads are in the sand. They really believe it takes sophistication. Readers of RISKS supposedly know better, although I have tried to be fairly gentle in exposing gross security flaws in existing systems. PGN]

Someone really sophisticated, with a Ph.D...

"Keith F. Lynch" <KFL@AI.AI.MIT.EDU>
Mon, 24 Mar 86 22:06:43 EST

There was a story on the front page of the Washington Post on February 20th headlined "Maryland Computer Whiz Kid Faces Seven Theft Charges" and subsubtitled "Credit Card Numbers Shared Electronically". It described a 15 year old who got credit card numbers off a pirate CBBS and ordered computer equipment over the phone to be sent to a vacant house. Other than this, the "whiz kid" did nothing at all remotely exceptional.

It looks to me like the wave of computer hysteria still hasn't passed. One of our Senators here in Virginia is introducing a bill to allow unlimited government snooping into personal computer files on the grounds that there might be data on child molestation (!) on the floppies. Seems to be an equally good case could be made on those grounds for warrantless searches of personal papers, and any other violations of the Bill of Rights I can think of.

Computer security is the responsibility of system managers. There is a growing trend toward making microcomputers, often with no security systems at all, available over phone lines. Unknown phone numbers are NOT good security. Lots of kids dial numbers randomly searching for modem carriers.

And there can be NO excuse for not having important data backed up. To make frequent backups should be the first thing anyone learns about computers. And being able to easily and frequently save state is one of the most important things any program should do.

...Keith

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 2: Issue 35

Sunday, 30 Mar 1986

Contents

San Jose Library

Matthew P. Wiener <weemba@brahms.berkeley.edu>
Fri, 28 Mar 86 00:14:06 pst

From an article in the 27 March 1986 San Francisco Chronicle:

An employee of the San Jose public library "destroyed 16 days of records and garbled two weeks of circulation files." A supervisor had "neglected to create a backup file". 267,000 books are involved.

They expect 95.5 percent will be returned on time. That leaves 12000. 4000 are routinely returned late. The other 8000 are considered lost at a replacement cost of $10 each, or $80,000. About $18,000 in overdue fines will be lost.

The system was two months old. Training was still incomplete. Several employees will be disciplined.

The blunder might cost three new positions for next year, expected to be refilled after cut out by Proposition 13 budget cuts.

I have one remark on the above.

Not only does poor computer usage cause risks to everybody else, I think we should be concerned about workers who are forced to use unfamiliar systems and then are held responsible for the damage they did. Somehow it does not seem fair, but I believe this is becoming far too common.

San Jose Library

Ken Laws <Laws@SRI-AI.ARPA>
Thu 27 Mar 86 12:36:52-PST

... at the main library and 17 branches. ...

That's $2,000,000 worth of books unaccounted for. The library usually gets 95% back without sending out reminders, but with the publicity -- who knows? They really can't afford to replace even $100,000 worth, even if they knew what to replace.

Inter-system crashes

Rich A. Hammond at lafite.UUCP <hammond%lafite@mouton.ARPA>
Thu, 27 Mar 86 08:32:18 est

I worked in a hotel once when they were adding a new wing. The main water and electricity systems had to be turned off to connect the new wing. Management decided to do both at the same time so there would only be one interruption in service. The problem: Turning off the electric power caused the emergency generator to come on, but the generator was cooled by water which came from the main and ran into the drain, i.e., no recirculation. Of course there was no water, the generator engine managed to warp its head pretty badly before we shut it off.

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 2: Issue 36

Tuesday, 1 Apr 1986

Contents

Errant Clocks

Barry Shein <bzs%bostonu.csnet@CSNET-RELAY.ARPA>
Sun, 30 Mar 86 21:25:09 EST

A reasonable double check before setting the time is to have the program check the last time the file system on disk was stamped with (I assume almost all O/S's stamp the time on the disk.) Certainly on a re-start time should not have moved backwards, for example, and some motions forward should be viewed with suspicion (more than say, a few hours.) This at least can be used to set a lower and upper bounds before the system screams on the console. UNIX uses this, I am sure other systems either do or could easily. Of course, this just shifts us to a different authority, and we know that the crash that started this cycle just might have damaged the file system, well, I guess that is left as an exercise for the designer, but at least you get to trust yourself.

-Barry Shein, Boston University

Computer Illiteracy

Matthew P. Wiener <weemba@brahms.berkeley.edu>
Tue, 1 Apr 86 05:59:33 pst

I'd like to relate a phenomena that happened when I computerized my grading system some years back. It used to be I did everything involving grades by hand, and one summer I finally wrote the software to do it all on by machine. From my point of view this was wonderful. I thought it was useful from the students' point of view: I now passed out individualized summaries of what my records had, giving them a chance to correct any mistakes I made. But one subtle hitch occurred.

Traditionally, I let the students come in at certain appointed hours after the grades have been computed but before they have been submitted to correct any last minute errors. I also take the time to explain their grades and how they were computed. It doesn't always make them happy; I cannot be budged when it comes to my judgement calls. This last chance office hour can be quite unpleasant at times--so many students take their grades seriously to the most ridiculous degrees, and make all sorts of irrational/emotional appeals to get the better grade.

When I switched over, the following happened. I was teaching calculus for non-technical students for the third year in a row, so I was expecting the same student reactions at grade time--especially from the pre-meds. Instead, as soon as a student began his/her complaint, and I said, "OK, let's check the records here," I'd show them the computer printout and he/she would then acquiesce immediately. "Oh, so that is why I only got a B+." They were, of course, the exact same numbers that I could have written down by hand on the specially lined paper provided by the department.

At the time I was elated at this easy solution to the pesky student problem that I had just found. But looking back, I find this reaction disturbing, with possibilities that the new computer illiteracy is actually dangerous to its victims.

Since then, the only students I've had who aren't put off by the computer printouts are the ones with actual computer experience and/or actual human intelligence, which usually occurs in the more advanced math classes.

> [We took this one, but let's go slow on starting a sequence of anecdotes on people trusting computers absurdly. There are enough cases to fill up the RISKS Forum forever. The message is clear, however. There is a lot of ignorance in the general populace. But do we really know better?
>
> Perhaps we should pervert the negative Turing Test hypothesis to "You can always tell a computer, but you can't tell it much." PGN]

San Jose Library

Dick Karpinski <ucsfcca.UCSF!dick@ucsf-cgl.ARPA>

Mon, 31 Mar 86 03:50:38 PST

Considering the amount of loss, perhaps some expert tinkering (a la NSA) could actually recover the info. I know we got data off _physically_ crashed hard disks through Data Recovery in LA a couple of years back.

Considering the forum here, perhaps I should mention the crashes we had. It was Fourth of July when they told me the PDP-11/70 would not boot. When I asked, they said one of our three 300MB drives blew a fuse so they had switched the pack to the center drive normally used for backups. Not only did the live data get trashed, but all three generations of our backup packs had been crashed between the time the backup was done and the time the pack was replaced with the next in cycle. Three weeks worth or so, switching packs in mid day and backing up at 4am. It took thousands of dollars and two weeks to get our data back. We gained new respect for inter-media backups and for fixed media disks.

Dick

San Jose Library

<Holleran@DOCKMASTER.ARPA>
Tue, 1 Apr 86 09:32 EST

If the public realized that the audit trail for returned books, records, tapes, et cetera was missing then more of the returned books, records, tapes, et cetera would not be returned. Most people return items on time or not unreasonably late only because there is an audit trail. Without the audit trail, there is no incentive for timeliness. A possible solution might be to lie and say to the newspaper that the audit trail had been recovered. As a follow-up, the library could then offer a penalty free time for the return of all materials.

Psychological and sociological consequences

Dave Benson <benson%wsu.csnet@CSNET-RELAY.ARPA>
Mon, 31 Mar 86 21:28:13 pst

(An inquiry from)
HARALD BAERENREITER, Fernuniversitaet, Arbeitsbereich Allgemeine
Soziologie, Postfach 940, D-5800 Hagen, F.R.G.

Regarding the inquiry from Baerenreiter: The light reading

Stephen Levy
Hackers: Heroes of the Computer Revolution
Doubleday & Co., 1984
(paperback: Dell Publ Co.)

should suggest some of the psychological and sociological risks associated with certain forms of computer use.

Please do note that I specifically disclaim any suggestion that computer
use CAUSES these psychological or sociological effects. It may well be that
certain psychological states induce the forms of computer use mentioned in
Levy's book. Whatever the case, the book is certainly enjoyable reading.

More inter-system crashes

<ihnp4!utzoo!henry@seismo.CSS.GOV>
Tue, 1 Apr 86 22:16:18 EST

Rich Hammond writes, in part:

> ...The problem: Turning off the electric power
> caused the emergency generator to come on, but the generator was cooled by
> water which came from the [shut off] main...

Apparently there were quite a number of vaguely analogous situations in
the Eastern Seaboard blackout of 1965. Samples:

One hospital had an excellent emergency generator that cut in promptly, but
it was in the basement. The hospital was in a low-lying area, and the
basement was kept dry by constant pumping. You guessed it: the pumps were
not on the emergency power bus, and the emergency power died as soon as
the rising seepage reached the generator.

Another organization (hospital?) discovered the hard way that its diesel
emergency generator had an AC-powered electric starter.

Most modern power plants need housekeeping power to function, and in
particular to start up. With the whole grid down, a chicken-and-egg
situation developed very quickly. The New York area got startup power
from a little power plant on Long Island, whose alert operator had
violated standing orders and simply opened all the circuits -- including
the power-grid tie-line -- when his meters went wild as the grid collapsed.
Boston got startup power from MIT; the MIT EE Dept. generators had been shut
down for the day, but apparently the MIT people managed to put together
enough car batteries (!) to bootstrap themselves.

Practically the only people whose emergency preparations really did work
flawlessly were the professional paranoids: the military and the phone
company. Even the air traffic control centers were dead; it was just as
well that it was a clear night with considerable moonlight.

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

COMPASS 86: A Progress Report

Al Friend <friend@nrl-csr>

Tue, 1 Apr 86 11:21:56 est

(From: Albert W. Friend, SPAWAR, Washington, DC)

The preparations for COMPASS 86 in Washington, 7-11 July are going quite well. Many people have expressed considerable interest in the keynote address by Dave Parnas:

When Can We Trust Software Systems?

We have received a number of abstracts and papers.

We should have an excellent attendance, based on the statements of those who say that they plan to come.

In reviewing the papers that have come in, we would like to see more papers in the areas of:

Measuring,
Assessing,
Specifying, and
Eliminating

risks due to defects in software, computer hardware design, process security, etc. We would be particularly interested in more papers from the academic community, especially ones with a strong basis in the theoretical infrastructure of software engineering, mathematics, etc. Also, papers relating to the psychology of programmers, and the possible limitations placed on practical software, would be extremely interesting. We have not even one paper in this area so far.

If you have any bright ideas, COMPASS is the place to try them out.

Any abstract received by Monday, 21 April will be reviewed by the program committee. They should either be sent by U.S. Mail to:

COMPASS, P.O.Box 3815, Gaithersburg, MD 20815

or sent to me over the net at friend at nrl-csr

Albert W. Friend, Program Chairman, COMPASS 86

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 2: Issue 37

Sunday, 6 Apr 1986

Contents

Request for information about military battle software

Dave Benson <benson%wsu.csnet@CSNET-RELAY.ARPA>
Sat, 5 Apr 86 17:06:18 pst

The following is an excerpt from a report of the talk by David Parnas, Lansdowne Professor of Computer Science at the University of Victoria and consultant to the Naval Research Laboratories in Washington DC. The talk was a list of reasons for why the envisaged SDI BMD software can never be trusted to work. The full report appeared recently on the arms-d bulletin board. To me, the most telling point reported is contained in the following exerpt from the report of the talk:

> --
>
> The other members of the SDI advisory panel that David Parnas was on and other public figures have said "Why are you so pessimistic? You don't have any hard figures to back up your claims." Parnas agreed that he didn't have any until he thought of the only one that he needed: ZERO. ZERO is the number of real systems that were trustworthy at first use. ZERO is the number of real systems that met unknown requirements at first use. ZERO is the number of prototyped systems that worked at first use. ZERO is the number of simulated systems that worked at first use.

ZERO!

To set the context, Professor Parnas is discussing military battle software in the above, or so the report leads me to believe.

Question: Can anyone offer evidence of military battle software which belies any of Professor Parnas' claims as reported above? Does anyone know about software which belies any of Professor Parnas' claims, even if they cannot, for security or other reasons, provide evidence?

I would greatly appreciate learning of such.
E-mail address: benson.wsu@csnet-relay
Postal service address: Professor David B. Benson, Computer Science
Department, Washington State University, Pullman WA 99164-1210, USA

Thank you very much for whatever information you can provide.

Programming productivity

<ihnp4!utzoo!henry@seismo.CSS.GOV>
Fri, 4 Apr 86 07:52:30 EST

In the course of catching up with a backlog of reading, the October 1985 issue of SEN (the ACM SIGSOFT newsletter) came to the top of the pile. Among its contents is an informal report by Jim Horning on his visit with a committee assessing the solvability of the SDI software problem. What I found most interesting was his report of a comment by one of the folks, Lipton I think, to the effect of "The physicists, given a few billion dollars, are quite willing to commit themselves to improvements of several orders of magnitude in laser efficiency. The computer science community is unwilling to suggest even one or two orders of magnitude improvement in the software-production problem." Granted that the comparison is not really entirely fair, this still got me thinking.

I went and re-read Terry Winograd's old "Reactive Engine" paper. He comments, roughly: "If, by decree of God or ARPA, we were only allowed to run one user at a time on the PDP-10, just think of all the effort that would be invested in making that one user's time productive." Despite the enormous increases in computing power available to individual users since then, that has not happened: much of that extra power is simply being thrown away. Most of the millions of personal computers out there spend most of their *active* time (when a user is actually seated in front of them using them) idling. Even the LISP machines are a pale shadow of the sort of thing that Winograd's observation calls to mind.

The other thing that came to mind was the genesis of the "Chief Programmer Team" in the "super-programmer" experiment at IBM. The key fact about the C.P.T. approach is that it was *not*, in its original form, a team at all: it was a support system for a single programmer. Consider the elaborate support setup that surrounds, say, a top trial lawyer: assistants, clerks, information-retrieval specialists, etc., all there to make sure that the central figure can spend his time using his unique abilities, rather than squandering endless hours on chores that don't require such skill.

How many programmers, even ones working on life-critical software like airliner flight control or fiercely difficult problems like ballistic-missile defence, have the kinds of electronic and human support that these thoughts suggest are possible?

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

Space Shuttle Software

Peter G. Neumann <Neumann@SRI-CSL.ARPA>
Sun 6 Apr 86 11:54:20-PST

In another post mortem on the Challenger explosion, the 6 Apr 86 SF Sunday Examiner & Chronicle ran a Chicago Tribune story on the presidential commission finding "a tangle of bureaucratic underbrush":

> "Astronauts told the commission in a public hearing last week that poor organization of shuttle operations led to such chronic problems as crucial mission software arriving just before shuttle launches and the constant cannibalization of orbiters for spare parts."

Open-and-Shut Case Against Reagan's Command Plane

the tty of Geoffrey S. Goodfellow <Geoff@SRI-CSL.ARPA>
4 Apr 1986 11:47-PST

SAN BERNARDINO, Calif. (AP) - When President Reagan comes to California for vacation, thousands of homeowners lose their automatic garage door openers to the interests of national security, a businessman says.

Larry Murdock, owner of Genie Garage Doors in San Bernardino, says he's certain that high-powered radio transmissions from the president's airborne command post jam the signals of the remote-control switches that open and close garage doors.

Murdock said Thursday he'd had 800 or 900 calls since Reagan arrived Sunday for a vacation at his Santa Barbara ranch. The E-4B plane is parked about 10 miles south of here at March Air Force Base.

Press officers for the Air Force and Secret Service would neither confirm nor deny knowledge of garage-door problems.

''We are concerned the president is in a safe and secure environment, and that plane is just that,'' Secret Service spokesman Bill Corbett told the San Bernardino Sun.

Re: Computer Illiteracy

Matt Bishop <mab@riacs.ARPA>
2 Apr 1986 0804-PST (Wednesday)

(This follows Matthew Weiner's message in Risks Vol. 2, No. 36)

This underscores a problem a lot of people have with computers -- they tend to regard them as "infallible." I always try to plant some seeds of doubt when I talk to people like that -- when I opened my bank account, the person at the bank did a quick electronic check to see if I was in trouble financially (she didn't call it a credit check when I asked.) While the box buzzed, I asked where it got its information, and she said she didn't know but was certain "the computer" was always accurate. She was quite surprised when I laughed and explained that that is not necessarily true. We talked about it, and her comment was, "Great -- now I'll always wonder if the computer's right whenever I do this check."

Maybe someday people who use computers (as opposed to those who program them) will learn not to trust them completely.

Matt Bishop

[By then there wouldn't be any computer jobs left. AI programs will do everything, including being the users, and we can all go down to the seashore. But we probably wouldn't be able to go in the water. PGN]

Search RISKS using swish-e

Search RISKS using swish-e

THE RISKS DIGEST

Forum on Risks to the Public in Computers and Related Systems

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

Volume 2: Issue 38

Wednesday, 9 Apr 1986

Contents

The UK Driving Vehicle Licensing Centre

Brian Randell <brian%cheviot.newcastle.ac.uk@cs.ucl.ac.uk>
Tue, 8 Apr 86 12:03:45 gmt

Several newspapers and magazines here have carried stories about
the alleged activities of hackers regarding the Driving Vehicle Licensing
Centre - a very large computer system that has received much bad
publicity in the press and in parliament over the years because
of cost over-runs and delays.
Here is a sample, from the April 1986 glossy journal "Business":

> "Computer hackers have been running a brisk racket "cleaning up" the
> driving licences of wealthy business men. For a charge of [pounds] 100
> a point endorsements have been erased from the files of the British
> Government's Licensing Centre at Swansea and its supposedly impenetrable
> computer ordered to issue new licences. Drivers who accumulate 12 penalty
> points within 3 years are liable to ban or disqualifications. Reckless
> driving, for instance, attracts 10 points; failing to stop after an accident
> 5.9 points; drunken driving 10 points (plus a 12 months disqualification).
> Drivers' records at Swansea are held on the Department of Transport's
> 3081 Model G mainframe, whose manufacturers, of course, are not responsible

> for its customers security procedures. About a year ago, an access code number appeared on at least four "bulletin boards" - informal computer games and information exchange facilities set up and used by home computer enthusiasts (not in this instance mischevious schoolboys).
>
> "I am not suggesting the number on the board was that of the DVLC", says a source, "but it gave you access to a database with levels of password protection. It was obviously a secure system and was related to DVLC because the name headed the file. The access was not very privileged but knowing the procedures allowed priority in the system and enabled you to eliminate endorsements and order new licences to be issued."
>
> Amendments to the DVLC mainframe were automatically carried through to the back-up records kept on magnetic disc storage."

Such stories have inspired denials from the DVLC - for example in Datalink:

> "The Driving and Vehicle Licensing Centre in Swansea has denied press reports that computer hackers have broken into its database and wiped traffic offenses off driver records.
>
> The DVLC, which employs 1500 staff in a computer centre running a variety of kit including two IBM 3083s, is adamant that its system is secure from outside interference. "We have no dial-in facility, there's no electronic access at all from off-site," a spokesman said.

Some 160 programmers work at the DVLC, and the spokesman admitted that officials are "looking at internal arrangements" to see whether files have been amended in return for payment."

My cynical view is that from most other sources such a denial would be immediately accepted, and indeed it may well be true. However the thought that such record tampering just might be going on, and so allowing banned drivers back onto the roads, is a worrying one.

Cheers, Brian Randell - Computing Laboratory, University of Newcastle upon Tyne

ARPA : brian%cheviot.newcastle@ucl-cs.arpa
UUCP : <UK>!ukc!cheviot!brian
JANET : brian@uk.ac.newcastle.cheviot

computer crime wave

<Hibbert.pa@Xerox.COM>
Wed, 2 Apr 86 10:53:29 PST

There was an article in the March 31, 1986 edition of the Washington Post's National Weekly Edition titled "The Computer Crime 'Wave': It's more politician's bark than our byte".

After an initial few paragraphs in which the writer reminded us that "national commissions that are set up to study and report on This Trend or That Issue always end up concluding that the trend/issue in question is a bigger national problem than anybody ever imagined", the article reported on the "First Annual Statistical report" from the National

Center on Computer Crime.

"Over a two year period, the national center surveyed 130 prosecutor's offices in 38 states and asked how many computer crimes each office had encountered. ... The national center's survey of prosecutors came up with a grand total of 75 reported 'computer crimes.' Even that minuscule number, it must be noted includes some infractions that can only be classified 'computer crime' if you stretch the language considerably. One reported case involves ... a county prosecutor ... who got a friend in the motor vehicle department to delete two speeding tickets from his driving record. This is labeled 'computer crime' because the record was on a computer tape...

In short, this first national census says that 'computer crime,' by any stretch of the definition, is a statistically minute phenomenon. The antics of a few hackers have garnered grossly disproportionate attention from the media and the law-enforcement community. So-called 'computer crime' is novel and exciting, so it's hardly surprising that even a few cases would attract considerable notice.

But Legislators around the country are acting as if there really is a 'computer crime' problem. The center's study shows that 22 states passed new 'computer crime' legislation in the past two years. ..."

Chris

Programming productivity

<LIN@XX.LCS.MIT.EDU>
Sun, 6 Apr 1986 23:45 EST

> From: ihnp4!utzoo!henry at seismo.CSS.GOV
>
> I went and re-read Terry Winograd's old "Reactive Engine" paper. He comments, roughly: "If, by decree of God or ARPA, we were only allowed to run one user at a time on the PDP-10, just think of all the effort that would be invested in making that one user's time productive." Despite the enormous increases in computing power available to individual users since then, that has not happened: much of that extra power is simply being thrown away.

True enough. But why do you think that large amounts of effort invested would necessarily improve productivity? Despite long practice, for example, people can hold only a few ideas simultaneously in short term memory. There are mnemonic aids available, but they don't enable someone to do hundreds of times better.

I use this analogy because there is some evidence that limitations on short-term memory account for a variety of cognitive limitations, among which may be programming. Ultimately, it may the limitations of the human mind that prevent us from forever expanding our achievements.

> How many programmers, even ones working on life-critical software like

> airliner flight control or fiercely difficult problems like
> ballistic-missile defence, have the kinds of electronic and human
> support that these thoughts suggest are possible?

That's easy. Not many. Indeed, military software procurement is by all accounts an utter mess.

Request for information about military battle software

Scott E. Preece <preece%ccvaxa@gswd-vms>
Mon, 7 Apr 86 09:43:05 cst

> [Parnas, quoted by Dave Benson]

> The other members of the SDI advisory panel that David Parnas was on
> and other public figures have said "Why are you so pessimistic? You
> don't have any hard figures to back up your claims." Parnas agreed
> that he didn't have any until he thought of the only one that he
> needed: ZERO. ZERO is the number of real systems that were trustworthy
> at first use. ZERO is the number of real systems that met unknown
> requirements at first use. ZERO is the number of prototyped systems
> that worked at first use. ZERO is the number of simulated systems that
> worked at first use. ZERO!

There are two essential, undefined terms in this statement: "first use" and "worked". The shuttle Enterprise, for instance, worked the first time they dropped it from its carrier 747. Was that its "first use", or do you count the many hours of simulation preceding that first flight? I wasn't there and have no idea whether there were bugs that showed up, but they clearly didn't keep the test from succeeding. Is that "working"?

The trouble with a debate like this is that it tends to force people more and more into idiotic dichotoomized positions. SDI software would obviously be a huge challenge to produce and validate. I have no hope it would work perfectly the first time used; I have no reason to believe it wouldn't work partially the first time it was used. The question of how perfectly it has to work is the central one. All the reports I've seen on both sides, including Parnas's essays, are hand waving. The task is too ill defined to be making statements about whether it can be done. The debate is silly. If you build the thing, you don't trust your security to it until you have been damned well convinced that it works; I am unwilling to accept the statement that "You can never be convinced that it works," when daily we all trust our lives dozens of times to things that we have been convinced work. There are plenty of good and, I think sufficient, arguments for not building SDI without claiming that it can't be done.

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

Aviation Week Technical Survey: AI & Aviation

Werner Uhrig <CMP.WERNER@R20.UTEXAS.EDU>
Tue 8 Apr 86 11:06:41-CST

[I am sure, readers of AVIATION and RISKS are interested also;
  for somewhat different reasons, of course ....   ---Werner]

Date: Wed 26 Mar 86 09:08:28-PST
From: Oscar Firschein <FIRSCHEIN@SRI-IU.ARPA>
Subject: Aviation Week Technical Survey

AILIST readers might be interested in the following:

Aviation Week and Space Technology, Feb. 17, 1986 has a technical survey of artificial intelligence, mostly applied to military applications. Included are the DARPA-supported programs in Pilot's Associate and the Autonomous Land Vehicle (ALV) and the VLSI lisp machine being built by Texas Instruments.

Company profiles include McDonnell Aircraft's work in the Pilot's Associate and avionics maintenance expert system; Boeing's AI Center; MITRE's work in natural language understanding; Grumman's decision support systems; Hughes AI center; and Westinghouse avionics troubleshooting expert system.

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 2: Issue 39

Friday, 11 Apr 1986

Contents

$36 million accounting mistake

Graeme Hirst <gh%utai%toronto.csnet@CSNET-RELAY.ARPA>
Thu, 10 Apr 86 12:10:32 est

[From the [Toronto] Globe and Mail, 10 April 1986]

BLUNDER BY ALBERTA COMPUTER LEADS TO $36 MILLION MISTAKE

A botched computer operation jeopardized the [Canadian province of] Alberta Government's ability to keep track of vehicle licence revenue, causing $36 million too much to be reported in a bank balance, the province's Auditor-General reported yesterday.

The Solicitor-General Department's new motor vehicles computer system was designed with little help from department accounting staff, an omission which ``undoubtedly'' led to many of its weaknesses, said Auditor-General Donald Salmon.

The division's bank balance was shown at $48 million on March 31, 1985, when it was actually $12 million.

In addition, the vehicles division lost track of accounts which could not be immediately processed, and unearned revenues were misstated by $2 million in March of 1985.

``These and other ancillary problems were caused largely by insufficent direction and control by senior financial management,'' the report said.

The Auditor-General picked up similar problems in 1981-82 in a massive new computer system developed to keep track of about $2 billion a year in natural gas royalties.

Oil revenues were miscalculated in a confused federal-provincial transfer of information involving three different price categories under the old regulated pricing system.

The governments later agreed to forget it rather than try to sort out the mess.

``The province didn't lose money,'' Mr Salmon said. ``You could probably say the producers lost some . . . but we did not quantify.''

Admissability of computer files as evidence?

Kathryn Smith <kathy%gsg.UUCP@harvard.HARVARD.EDU>
Thu, 10 Apr 86 12:02:39 est

This arises out of a discussion in mod.legal over the meaning of UNIX as a trademark, and how it (the name) might/might not pass into the public domain by becoming a generic descriptive term for a type of operating system rather than refering to a specific product of AT&T. One of the postings which I quote below raised the broader question of the use of postings to a computer network as evidence.

In a recent posting (Message-ID: <8604011618.AA15083@bu-cs.ARPA>), Barry Shein said the following:

> "What immediately occurs to me is that if I were an ATT lawyer I would squirrel away the note imploring people not to attribute UNIX as a (whatever) of (whomever.) It could prove very useful to open an argument that any appearance of it coming into common use was in fact a conspiracy on the part of the technological community."

I have no idea of the likelihood of the "conspiracy" defense working to hold onto AT&T's trademark, however the part about holding onto the note got me to thinking. Does anyone out there know if any precedents have been set for the admissability/inadmissability of computer files as evidence in court?

I, for one, find the thought that some court of law might, in ignorance, accept computer files as evidence frightening. Certainly on UNIX if you can get access to a privileged account, whether legally or illegally, you can change anything on the system, including editing i-node entries to alter creation dates, etc., with no way I can think of of proving that alterations were made unless the hacker does something extra-ordinarily stupid. I suspect that the same is true of most other systems. No matter how good system security is, given sufficient knowledge of how it works, it is breakable.

Coupled with the unfortunate tendency of the layman to accept whatever comes out of a computer as gospel, this provides some very strong reasons for not trusting computer files as evidence, but considering the growing number of transactions being performed by/on computers, there are, or soon will be, a great number of areas where the computer's audit trail may be the only evidence of a transaction. Have any precedents been set already, and if not, what do people think the solution is?

Kathryn Smith
(...decvax!gsg!kathy)
General Systems Group
Salem, NH

[This is a very valid question. The crypto community has all sorts of techniques for crypto sealing for integrity and crypto authentication. Reasonable techniques exist to give some better assurance, but there are always going to be some internal vulnerabilities. However, since most legal and administrative people do not yet recognize the ease with which on-line evidence -- including audit trails -- can be altered, and for other reasons as well, these techniques are not yet in widespread use. PGN]

"Rapid advance" of SDI software

<thode@nprdc.arpa>
9 April 1986 0807-PST (Wednesday)

In an article in the Sunday San Diego Union, Gregory Fossedal (Copley News Service) discusses the "rapid advance of SDI." He indicates that progress is good enough that a "decision to deploy a Star Wars defense ... could be made before Ronald Reagan leaves office." He describes some progress made in lasers and other hardware areas. He then goes on to discuss progress by software engineers, and says that "concepts in computer software ... have leaped ahead." He indicates that critical arguments "...that 'a single error' could cripple the whole shield apply only to outmoded types of unwieldy, highly centralized software. Thanks to new software ideas, Star Wars defenses need not be run by a grand central brain."

--Walt Thode (thode@nprdc)

[Announcements of great BREAKTHROUGHS often coincide with great BREAKDOWNS -- in communication and common sense. This one is being hyped like a great BREAKFAST cereal -- distributed Wheaties are better than old Wheaties, the breakfast of chumpions. Don't put all your eggs in one basket -- just use thousands of baskets instead, and train the hens to

BREAKDANCE in space. But don't forget to distribute the roosters as well. Walt, thanks for the enlightenment.

I note that in principle there are indeed some software engineering advances, but nothing that GUARANTEES that distributed systems are sound -- especially in their operating environments. The tradeoffs are very complex, and thus this is not a simple discussion. Many problems of centralized systems reappear in other guises in distributed systems, and wonderful new problems arise. Perhaps some day we will have a dispassionate, technically motivated analysis -- although many of the arguments are nontechnical. PGN]

Blame-the-computer syndrome

<JANLEE%VTCS1.BITNET@WISCVM.WISC.EDU>
Wed, 9-APR-1986 09:37 EST

One of my colleagues, a visiting prof. from the UK, bought a new Ford Escort in mid-February and at the same time purchased the "Extended Warranty" package. Following a trip to Florida for Spring break, the vehicle broke down outside Daytona (that may suggest this is a put-up job!!) on Saturday afternoon March 29th (also Easter Weekend). Calling the 800 number he was referred to a specific repair shop. On arriving there the owner called the 800 number to confirm the warranty and was told that there was no record of a warranty "in the computer" and that any additional enquiries would have to wait until Monday. They stayed in a hotel over the weekend (at a high rate since they had no reservations and limited means of transportation) and on Monday were again informed that there was no record of their warranty. It took most of the rest of that day to have the dealer from whom they purchased the car to confirm that ARTh a warrenty did exist and to have the repair shop agree to START the repairs. It turns out that the dealer doesn't send in the warranties until the end of each month, and the backlog doesn't allow the warrantor to get them in the computer for perhaps another month. This is probably based on the probability that a new car won't need repairs in the first two months and in any case the owner would probably be close to home still! Here is a typical case of having a computer in the system and thus being able to "hide" behind it. By the way, check you own extended warranty to see if it covers the cost of hotel accomodations!

Also, I am still researching the Melbourne Bridge Failure for you -- I have got the sequence of events and a precis of the findings of the Royal Commission which blamed the failure on a computer program, but I am waiting for a copy of the actual report before I send you more. The sequence of events is well documented in the London Times but I am not sure I want ot trust their reporting on this about the program use until I see the report.

JAN

PS. Did you see the Hackers Report in CACM this month? [Yup. Arrived today.]

Hackensack Phone Snafu

Dirk Grunwald <grunwald@b.CS.UIUC.EDU>
Thu, 10 Apr 86 16:04:50 CST

According to a NYT article reprinted in the Daily Illini, a local student newspaper, the phone system in Hackensack N.J. experienced a problem with billing long-distance phone calls from pay-phones. I quote:

> Technology in an electronic switching center here failed New Jersey Bell, and for nearly two months perhaps half the international calls placed from 400 pay phones around town went through without charge, according to Ted Spencer, a spokesman for the company.
>
> ``Apparently a problem developed in a computer program - in the software,'' Spencer said. ``We don't have a record of the calls that got through. They bypassed the billing system.''

Does anyone have anymore in-depth information concerning this? Several people who used the loop-hole were arrested and charge with theft of services.

Dirk Grunwald, Univ. of Illinois

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 2: Issue 40

Saturday, 12 Apr 1986

Contents

GREAT BREAKTHROUGHS [Red Herrings swimming upstream?]

Peter Neumann <Neumann@SRI-CSL>
Fri, 11 Apr 86 07:34:38 pst

In this issue of RISKS, we include a commentary on the article by Fossedal, contributed to me privately by Dave Parnas, reproduced with his permission.

>In an article in the Sunday San Diego Union, Gregory Fossedal (Copley
>News Service) discusses the "rapid advance of SDI.".... He then goes on to
>discuss progress by software engineers, and says that "concepts in
>computer software ... have leaped ahead." He indicates that critical
>arguments "...that 'a single error' could cripple the whole shield apply
>only to outmoded types of unwieldy, highly centralized software. Thanks
>to new software ideas, Star Wars defenses need not be run by a grand
>central brain."

Message from Dave Parnas follows:

One of the more amazing aspects of this report is that no plan ever called for the defenses to be run by a "grand central brain". If you read the unclassified volume of the Fletcher report, you will find a proposal for a highly decentralized distributed system. The Fletcher panel worried about the survivability of the system and proposed a system in which each battle station could function on its own if others were destroyed. They even rejected a military-like hierarchical command structure for the computers so that there would be no "Achilles Heel" in the system. Nothing that I have read ever proposed a centralized system.

When the SDIO Panel on Computing in Support of Battle Management (PCSBM) announced that people were assuming a highly centralized system as per the Fletcher report they were using a classic political technique, the "red herring". The Fletcher panel was not anywhere near as stupid as they implied. I have not seen the contractor designs but I cannot believe that they were as stupid as was suggested either.

Some of the newspaper reports on the PCSBM red herring suggest that there is a proposal to build a network in which the battle stations remain autonomous by having no communication. That is simply not the case. Every report that I have seen calls for extensive communication between those stations. Weapon Stations that were denied the use of data obtained by other satellites would be severely handicapped and more easily defeated.

Fossedal's reference to "a single error" is part of another red herring in which SDIO supporters claim that the critics want perfection. The only reference to "error free software" came from SDI supporters, none of the critics have assumed that perfection was needed. You only have to get rid of the errors that matter. Some claim this as a new discovery as well.

When Fossedal reports such great progress, it is progress from a position that was never held by any responsible computer system designer.

[End of message from Dave Parnas]

Military battle software

James M Galvin <galvin@dewey.udel.EDU>
Thu, 10 Apr 86 15:52:59 -0500

> From: preece%ccvaxa@gswd-vms (Scott E. Preece)
> Date: Mon, 07 Apr 86 09:43:05 -0600.
>
> There are two essential, undefined terms in this statement: "first use"
> and "worked". ...

What about your essential, undefined phrase "convinced that it works"? In the context of your argument I assume you are being facetious, but it is not clear. I will agree with you if what you are saying is that "convinced that it works" is really just a "small probability of failure". True, I trust my life to my car every day, but who's to say that someday the steering column won't fail.

The next question is how small a probability is desired and how is it achieved? Isn't that an essential component of Parnas' argument?

Jim

Herb Lin <LIN@MC.LCS.MIT.EDU>
Sat, 12 Apr 86 14:39:15 EST

| From: preece%ccvaxa@gswd-vms (Scott E. Preece) [...]
| There are two essential, undefined terms in this statement: "first use"
| and "worked".

Actually, the meaning of first use for a missile defense system is
pretty clear -- it means the first time the Soviets launch an attack
on the U.S.

| The question of how perfectly it has to work is the central one.

Not true. The central question is how well you can know its
performance before it is called into action.

| If you build the thing, you don't trust your security to it until
| you have been damned well convinced that it works...

What would you consider sufficient to convince you that it "works"?
What evidence of "working" should the nation accept as "proof" that it
works? If there is no evidence short of an ensenble of nuclear wars,
then it is a meaningful statement to say that "you will never know".

Information about military battle software

Scott E. Preece <preece%mycroft@gswd-vms>
11 Apr 1986 08:58-CST

> The next question is how small a probability is desired and how is it
> achieved? Isn't that an essential component of Parnas' argument?

Yes, I think that's the essential question. I think Parnas is saying that
you can never prove adequately that the probability is sufficiently small,
so you might as well not work on the question.

I wear my seatbelt BECAUSE there is always a probability that my steering
will fail or the wetware guiding some other vehicle will fail. I know there
is also a small probability of the seatbelt failing, too, but there the risk
is low enough for me to accept. If I could have airbags in a car I could
afford, I would.

I don't know if it is possible to build software systems capable of dealing
with the problems inherent in SDI. I don't know what level of testing and
verification would be necessary to convince me that the software (and the

hardware) worked. I think Parnas is saying that it IS impossible to do and that NO proof could be sufficient. I think that's wrong headed.

There are perfectly good arguments against going ahead with SDI -- destabilization is sufficient in itself, cost and the false sense of security are also strong arguments. Short range submarine-based missiles, cruise missiles, and emplaced weapons are further arguments.

I think the Parnas arguments are tangential and misleading. He creates a situation where every time someone says "But look at system X; it worked fine when it became operational" it becomes an argument for the pro-SDI side. Somebody (Asimov? Clarke?) has said "Whenever a very senior scientist says something is impossible, the odds are he's wrong." That's the way I react automatically to Parnas's arguments. I think a lot of other people do, too.

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

Preece's msg, first-time software, and SDI

Dave Benson <benson%wsu.csnet@CSNET-RELAY.ARPA>
Wed, 9 Apr 86 23:56:33 pst

To keep the thread of the discussion, I quote liberally from Preece's msg to RISKS and comment on certain sections:

|Date: Mon, 7 Apr 86 09:43:05 cst
|From: preece%ccvaxa@gswd-vms (Scott E. Preece)
|Subject: Request for information about military battle software
|> [Parnas, quoted by Dave Benson]

Correction. This is from a report of a talk by Parnas. I believe it correctly represents Parnas' views, but may not be a quotation. I did not have the opportunity to listen to the talk. Pullman is 300 airmiles from Seattle. The full report appeared on the ARMS-D bboard.

|> The other members of the SDI advisory panel that David Parnas was on
|> and other public figures have said "Why are you so pessimistic? You
|> don't have any hard figures to back up your claims." Parnas agreed
|> that he didn't have any until he thought of the only one that he
|> needed: ZERO...
|
|There are two essential, undefined terms in this statement: "first use"
|and "worked". The shuttle Enterprise, for instance, worked the first
|time they dropped it from its carrier 747. Was that its "first use", or
|do you count the many hours of simulation preceding that first flight?
|I wasn't there and have no idea whether there were bugs that showed up,
|but they clearly didn't keep the test from succeeding. Is that "working"?

My interpretation: The simulation preceeding the first flight is not the "first use" I had in mind. The first operational use of real-time control software is. So your example is a good illustration of the working of first-use real-time control software with humans (pilots and ground personnel) in attendence. In the minimum sense that the Enterprise was piloted to a landing, the test was indeed a success. (It may have been a success in many other ways as well-- not the issue here.) So, the software clearly worked. Furthermore, at least the test pilots trusted it to work, so it is an example of a real system which was trustworthy at first use.

I appreciate having this example drawn to my attention. Over and over again I am impressed with NASA sponsored software, and this is another example of how well NASA software contractors have done their work. Any reader who has helped build NASA software should take pride in some of the finest real-time control software ever engineered.

However, my call was for military battle software. Landing the shuttle Enterprise does not qualify on these grounds. (It might not qualify on other grounds in that the purpose of the space shuttle is not to drop from the back of a 747 and land sucessfully. This was only a partial operational test of the flight software. The first full operational test was attempting to put the shuttle in orbit. If I recall correctly, there was a synchronization fault in the sofware... I don't want to quibble.)

If some of you have other NASA real-time control software stories to contribute, especially if you are willing to make a judgement about how well it worked the first time, I would greatly appreciate reading your contributions. Please send them directly to me, unless you think the stories have relevance to the purposes of the RISKS bboard. Thank you. But what I am primarily looking for is military battle software experiences.

|The trouble with a debate like this is that it tends to force people
|more and more into idiotic dichotoomized positions. SDI software would
|obviously be a huge challenge to produce and validate. I have no hope
|it would work perfectly the first time used; I have no reason to believe
|it wouldn't work partially the first time it was used. The question of
|how perfectly it has to work is the central one.

I agree with the last sentence cited. In existing military battle equipment, when employed in realistic manuvers or in actual battle, there is a mission to be accomplished. If the mission is accomplished in the FIRST ATTEMPT, then this negates Parnas' claim. If the mission is not accomplished, his hypothesis stands. We see that Parnas' statement satisfies one of the criteria for a scientific hypothesis: It is rendered false by one experiment.

One could imagine situations in which the mission is partially accomplished. With the distructiveness of modern weaponry (and I'm not even including nuclear devices in this thought), it is usually possible for a disinterested judge to easily place such partial accomplishment in the Yea or Nay column. (However, no such cases have yet come to my attention, beyond Herb Lin's discussion of the Aegis test is his Scientific American article, December 1985 issue. This test is an obvious failure for the software. There were particular requirements which the software failed to meet.)

So I think it perfectly reasonable to attempt to collect data about actual military software, irrespective of SDI. Parnas has stated a strong, refutable claim. If you will, a testable hypothesis about the software engineering of military battle software. The only sort of experiment I can do is to ask whether any of you, whether any of your friends, peers, associates, know of any actual experience to the contrary. It only takes one such (reliable, honest) piece of such information to refute Parnas' claim. I'm still waiting.

I remain of the opinion that actual engineering experience teaches some important facts about the artifactual world in which we live. Our engineering successes, our engineering failures, eventually provide an understanding of what works and what does not. The successes and failures place the limits on our ability to understand, in an engineering sense, the real world. Put a bit more strongly than I really mean (but it will take a long essay to explain: See Petroski's book "To Engineer is Human"),

> Engineering is the design of artifacts, using the accumulation of knowledge about artifacts gained through experience with similar artifacts.

|The task is too ill defined to be making statements about whether it can be
|done. [The task being SDI battle software, dbb]

I beg to differ with this statement. Pick a mission, any mission for SDI other that the trivial one that SDI does absolutely nothing at all. This becomes the requirement for the battle software. So far there is no evidence that the SDI battle software would complete your mission on first operational use. There is only evidence that this battle software, like all battle software, would fail in the first operational use.

Therefore data, facts, about the first operational use of military battle software are relevant to the question of whether any nontrivial mission for SDI is possible in actual engineering practice. This data does make a difference in attempting to understand whether SDI battle software would or would not work the first time.

Thank you this opportunity to expostulate.

I remain, still waiting for data to refute Parnas' claims, Dave Benson

PS. Please send refuting data to benson%wsu@csnet-relay
Mail to: Professor David B. Benson, Computer Science Department,
Washington State University, Pullman, WA 99164-1210.

First use - Enterprise

"Lindsay F. Marshall" <ncx%cheviot.newcastle.ac.uk@cs.ucl.ac.uk>
Thu, 10 Apr 86 08:53:05 gmt

> [Two messages are collapsed into one, omitting my intervening request for clarification. PGN]

I must admit that regarding the first shuttle flight, I had heard that there was a serious computer failure immediately after the vehicle had been released.

This story comes from Jack Garman, via Tom Anderson. On the first glide test of the shuttle from the back of a 747 the first two messages on ground telemetry were : "Explosive Bolts Fired", "Computer No.3 Failed"

Lindsay

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 2: Issue 41

Sunday, 13 Apr 1986

Contents

Computer Naivete

"Lindsay F. Marshall" <ncx%cheviot.newcastle.ac.uk@cs.ucl.ac.uk>
Fri, 11 Apr 86 11:32:53 gmt

A LITTLE OFF KEY   [from the Guardian Computer Page April 10]

A member of our Moles in Schools project reports that an adviser was called to a school where they were having trouble with their new disc drive. He arrived to find a C15 cassette tape wedged firmly in the slot.

Then a headmaster reported that his school had "broken their BASIC". They had got a syntax error message.

Best of all was the school where staff took exception to the QWERTY arrangement and rearranged the keys to read ABCD etc. To their consternation the character on the key which had been hit did not then correspond to what appeared on the screen. The adviser was greeted, on arrival, by an eight-year- old boy saying: "Thank goodness you've come. They don't know what they are doing. I told them they had to change the switches underneath as well but they wouldn't take any notice of me."

Re: Admissability of computer files as evidence?

Scott E. Preece <preece%ccvaxa@gswd-vms>
Fri, 11 Apr 86 09:56:01 cst

> From: kathy%gsg.UUCP@harvard.HARVARD.EDU (Kathryn Smith)
> I, for one, find the thought that some court of law might, in
> ignorance, accept computer files as evidence frightening...

I would think that a computer file would be acceptable evidence under the same conditions that a paper document would be acceptable evidence -- when there was a believable evidentiary chain establishing its provenance. Thus a computer file bearing a particular date would mean just as little as a piece of paper with the same date, unless it could be established that that particular piece of paper was in a known place, under neutral or believable control, since that date. If I take my dump tape from this afternoon to a neutral agent and leave it there, I would expect a court at some time in the future to accept that everything on it at that future time was on it today. I would not expect the court to believe an arbitrary date BEFORE today on the tape any more than I would expect the court to believe the date on a paper letter from my files.

scott preece [gould/csd - urbana]
ihnp4!uiucdcs!ccvaxa!preece

[Lay people -- and even some of our colleagues -- tend to TRUST computers and ignore the people risks involved! But a tape can easily be forged -- unless some nontrivial authenticator (crypto seal?) is used. And even that can be forged with a little effort. Similarly, on-line files can often be changed without leaving any audit trail record of the change. Furthermore, detecting Trojan horses and viruses in the computer world is generally nontrivial. On the other hand, in the paper world the piece of paper without provenance is more likely to be suspect. Occasionally there may even be some evidence of tampering. The burden comes down to good audit trails and protocols for handling both computer data and paper, as well as anticipation of what might someday be subject to tampering -- possibly everything -- and treatment accordingly. But once again, there are no guarantees and many pitfalls. PGN]

Programming productivity

<ihnp4!utzoo!henry@seismo.CSS.GOV>
Fri, 11 Apr 86 10:38:46 EST

Herb Lin writes:

> ... But why do you think that large amounts of effort
> invested would necessarily improve productivity? ...

Remember "chunking". Cognitive limitations can often be bypassed by moving things to a higher level. Few people would ever write (say) C code if doing so required understanding the details of the compiler. One major thrust of the sort of support systems, both human and automated, that I was alluding to, is removing the need to attend to unnecessary detail.

We have already come a long way in this direction: much of the fundamental knowledge base of a programmer of thirty years ago is obsolete. Not just because the machines have changed, but because modern programming is done at a much higher level, where the low-level details are no longer visible.

Of course, the low-level details have not vanished; they have merely been taken over by the support systems. Which means that one must worry about whether the support systems understand the details properly. Although programmer productivity is much increased if one can work entirely in a high-level language and not have to care about the details of the underlying machine, one's compiler had better be fairly well debugged or this strategy will not work.

Even if one stipulates that ultimate limitations exist, it seems to me that there remains good reason for believing that we are nowhere near them yet, and that investments in better support systems are worthwhile now and will remain worthwhile for the foreseeable future.

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

The San Jose Public Library

Sriram Vajapeyam <g-vajape@gumby.wisc.edu>
Fri, 11 Apr 86 22:27:49 cst

```
<>From an article in the 27 March 1986 San Francisco Chronicle:
>              ------------------------------
>  An employee of the San Jose public library "destroyed 16 days of records
>  and garbled two weeks of circulation files."  A supervisor had "neglected
>  to create a backup file".  [...]
>  Training was still incomplete.  Several employees will be disciplined.
   ^^^^^^^^ ^^^ ^^^^^ ^^^^^^^^^^         ^^^^^^^^^ ^^^^ ^^ ^^^^^^^^^^^
>              ------------------------------
>Not only does poor computer usage cause risks to everybody else, I think we
>should be concerned about workers who are forced to use unfamiliar systems
>and then are held responsible for the damage they did.  Somehow it does not
                             ^^^^^^^ ^^ ^^^^ ^^^
>seem fair, but I believe this is becoming far too common.
 ^^^^ ^^^^
>------------------------------
```

Penalising the employees DOES seem unfair in the above case, and I feel they are sure to win if they go to a court of law seeking remedy. (They didn't have enough training; the system was very young; we don't know if the system was fully reliable; etc etc.) I have a few points about which others might want to express their opinions :

* Mistakes made while using computers result in much more loss than those made, say, when working with official documents on paper.

[This is influenced by the shorter time scale, the (misplaced) willingness to trust computers, and by the laziness/complacency of computer users in not spotting mistakes. But I'm not sure that your point is generally true. PGN]

* It seems easy for a person not very comfortable with computers to make mistakes that can't be corrected. (It doesn't seem fair to expect *everyone* to be comfortable with computers.)

* How reliable is it to use computers in cases such as above (e.g., banks, libraries, etc), when they will be handled by people who might be more prone to making mistakes? SDI, even though having been brought into existence and being maintained and used by professionals, is not supposed to be reliable. Human error is always a frightening possibility even there!

...Sriram V.   g-vajape@gumby.wisc.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 2: Issue 42

Monday, 14 Apr 1986

Contents

[Ron Cain <CAIN@SRI-AI.ARPA>: robot safety]

Bill Park <PARK@SRI-AI.ARPA>
Mon 14 Apr 86 13:22:55-PST

Mail-From: CAIN created at 14-Apr-86 09:19:46
Date: Mon 14 Apr 86 09:19:46-PST
From: Ron Cain <CAIN@SRI-AI.ARPA>
Subject: robot safety
To: IA.STAFF: ;

For those who hadn't heard, I thought I'd mention two close calls we had out in the welding lab a week or so ago. It is worth keeping them in mind the next time you stand near a robot.

In the first incident, a 68000 board in our system failed and caused the processor to jump to (of all places) a robot move routine. We were all standing around the emergency stop button looking at a terminal, and Jeff and Talia got to the button within a few milliseconds of hearing the crunching noise which marked the premature demise of a small jack belonging to the lab. With our sensor mounted on the end-effector as it was, it could have been alot worse if we had been further from a kill button.

The second incident was even more sobering. Some drive motor cards in the Cincinati-Milacon box failed and joints 5 and 6 began

jerking around randomly. Again, the kill button was nearby, and a
potentially disastrous situation (at least for the sensor) was avoided.
It could have been any other joint -- including the base or the shoulder.
And someone could have been standing next to it. We do all the time.
The point is just this: it can and does happen.
Watch yerselves around robots.
... ron

Re: Use of computer files as evidence (RISKS-2.39)

Rob Horn <decvax!wanginst!infinet!rhorn@ucbvax.berkeley.edu>
Mon, 14 Apr 86 13:28:33 est

The use of computerized data as evidence has been treated carefully in the environmental field (a litigious arena which includes acid rain, toxic wastes, etc.). The basic rule is:

Computer-based data is NOT evidence unless ALL parties involved agree to treat it as evidence.

Yet, almost all of the data acquisition and processing is performed by computers. The route around this that is used by the legal process is a dual PAPER or (only recently) MICROFILM evidence trail. Using this trail the following must be shown:

1). All instrumentation calibrations are traceable to NBS standards, with logs that are properly documented and signed by humans, in non-erasable ink on paper. (Also on numbered sheets in bound notebooks only, with countersigned dates and occasion Q/A checks).
2). The computer processing includes the processing of routine calibration so that the computer is part of the calibration loop.
3). All reports are provided in both computerized and hardcopy form. The hardcopy version is certified and signed by a Q/C person.
4). All equipment logs and records are duly signed and archived.

In fact, the computer records are generally trusted and used, but all significant evidence is verified against the paper trail. This does not prevent tampering, but it does introduce several levels of human verification and record keeping on top of the computer. The legal system is comfortable with its ability to deal with human error and dishonesty, so they switch to the human trail when in doubt.

These rules posed quite a problem in automating some of the data acquisition processes, because the people involved would NOT SIGN reports that they could not verify. (They had significant personal liability). Most of the reports had to be generated on the spot (so that the signer could verify that the equipment was behaving correctly), and include a hardcopy printout that showed all of the equations and intermediate computations used (so that the signer could double check whenever the numbers looked unusual or the value looked like it might have legal significance). Then from these individual data items computerized reports could be generated, but again the signers of those reports insisted on hardcopy for intermediate terms and double checked all the suspicious or signficant numbers.

Did mistakes get through? Probably. But the error levels were low and bad reports had a decent chance of being corrected. Disputed reports could be re-created by hand from "raw" data if necessary. The "raw" data being computerized instrumentation reports that were paper logged and signed.

Was the computerization complete? Definitely not. The people involved refused to sign reports from a program where they were unable to perform independent validation on a spot check basis, nor where they could not find a totally hardcopy re-creation path.

My experience in this is now four years old, but this area changes slowly and the rules are probably still the same. The people involved are very unwilling to abandon their independent audit path. They were only willing to trust computers for the general case, not the oddball or legally significant items. For things like averages, etc. they were willing to trust computers after verifying 5% (selected at random) by hand.

Rob Horn
UUCP: ...{decvax, seismo!harvard}!wanginst!infinet!rhorn
Snail: Infinet, 40 High St., North Andover, MA

Review of *Softwar*

Gary Chapman <PARC-CSLI!chapman@su-glacier.arpa>
Fri, 11 Apr 86 09:19:00 pst

I thought participants of Risks might be interested in a recently released book called *Softwar*, by Thierry Breton and Denis Beneich, two French computer professionals. The book is a computer science thriller, so for all of you out there who have longed for computer scientist heroes and heroines who resemble Indiana Jones or Mata Hari, this book is for you. (*Softwar is published by Holt, Rinehart Winston, and is available only in hardcover right now, at $15.95.)

The two principal characters in the book are computer scientists, one male and one female, one American and one Russian, who happen to have been lovers, too, of course. The American is Assistant Professor of Computer Science at MIT Brendan Barnes, who is an expert on software reliability and debugging. The Russian, who was a grad student at MIT, is Yulya Voronkov, a beautiful Soviet computer scientist who is one of the department heads at the main Soviet computing center in Krasnoyarsk in Siberia.

Barnes writes a piece for *Computers and Society* that talks about the potential of using software as a weapon in the ideological war with the Soviets. This piece naturally attracts the attention of the CIA, and Barnes is gently (and without much resistance) coaxed into becoming a member of a team of military officers, CIA agents and technical experts who plan to use software bugs to plague the Soviet effort to computerize their economy. They call these "softbombs," in a "softwar" with the Soviets. As one character puts it in one of the many extemporaneous speeches about the role of computers in national security:

...any sector of society can be destabilized, even completely paralyzed--industry and defense, civil and military communications, logistics and transport, public administration, the entire economy--simply by a couple of keystrokes on a computer terminal, anywhere in the world. We do definitely see this as the electronic battleground of the future, and we definitely see ourselves of being in the process of seizing the high ground for ourselves before the other side can get there.

Barnes and his colleagues start by sabotaging a piece of software bought by the Soviets from the French. It runs on a newly purchased "Craig 1" that the Soviets bought from the United States. The software is programmed to spit out garbage when the U.S. Naval Weather Station in the Virgin Islands reports a barometric pressure of 1230 millibars. Then it is programmed to restore all the data in perfect shape when the Weather Station reports that same figure again. Of course, the Naval Weather Station is instructed not to report that figure unless specifically told to do so, so the "softbomb" is detonated at the choosing of the CIA. They pick a detonation time about an hour before the "Craig 1" is to be demonstrated to a visiting delegation of the Soviet Academy of Sciences.

But, aha! There is a clever programmer at the console of the "Craig 1" who is bound and determined to find out why the machine went crazy at such an embarrassing time. He eventually discovers the programming trick, and is on to how this is the product of deliberate tampering by someone outside the Soviet Union. The KGB zeroes in on Professor Barnes, and he nearly catches a hand grenade in a Paris bar.

From there on out, it's a battle of wits between the American computer scientist and his Soviet counterparts, and of course gradually that becomes the gorgeous and brilliant Yulya, his former grad student and former lover.

The book is a fun read most of the time, especially for those intrigued by MIT trivia, Soviet trivia and computer trivia. There are a few too many spots where some character gives a speech about the importance of computers to some such thing or other (Barnes gives a long speech to his wife about why he's mixed up with the CIA and catching hand grenades in Paris and having an affair with a beautiful Carribbean journalist, and it turns out that he's a radical democrat who wants computers used to increase the democratic process in the West). But on the whole, it's a fairly conventional thriller spiced

up for computer professionals with lots of jargon and speculation, and of course, dashing, sexy and adventurous computer scientists.

-- Gary Chapman

"Computerized Voting -- No Standards and a Lot of Questions"

Ron Newman <newman@ATHENA.MIT.EDU>
Mon, 14 Apr 86 21:50:29 -0500

The following is a slightly edited version of an article I wrote for the April, 1985 issue of the Computer Professionals for Social Responsibility Boston Chapter newsletter.

~~~~~~~~~~~~~~~~

Our guest at CPSR/Boston's March 19 meeting was Eva Waskell, an independent science writer, former computer programmer, and current stringer for The Economist. She spoke with considerable alarm about the rapid and unregulated spread of computerized vote-counting systems in American elections.

Waskell became interested in computerized vote-counting when Severo Ornstein of CPSR National suggested that she look into several lawsuits pending against Computer Election Systems (CES) of California. CES is the leading vendor of such software; it estimates that approximately 25% of the U.S. popular vote is cast on its equipment. Losing candidates in three states have sued the company, claiming that its system produced inaccurate or fraudulent results. While investigating, Waskell was appalled to find out that only one person outside of CES, a consultant for one of the plaintiffs, had ever examined the code. Waskell's investigation resulted in several New York Times articles last summer.

To use a computerized ballot system, a voter inserts a punch card into a book containing the names of each candidate for office. The voter casts a vote by pushing a stylus through a hole in the book next to the name of the candidate. thus punching out the appropriate hole in the punch card. When the polls close, punch cards from all the precincts are trucked to a central location and tabulated on a mainframe, using software provided by CES or a competitor.

The first such system was developed by IBM in 1964, for use in Los Angeles elections. In 1969, there were accusations of fraud in LA's elections. Fearing unfavorable publicity, IBM got out of the election business. Four of IBM's employees left IBM to form CES.

Waskell pointed out four problems with this type of system:

1) A single central computer, in a single location, is counting all the votes. This takes control away from precinct poll workers, who formerly counted the votes and could recognize deviations from traditional voting patterns in their precincts. It also makes rigging the election much easier: instead of having to buy off many individual precinct workers, who are known to the community, one need bribe only a single computer operator, who is known by almost none of the voters.

2) Election officials must now be much more than clerical workers -- they must have technical skills. Frequently, new people are hired from the outside to learn and operate the computer equipment. Officials often do not know what the new people are doing. In one state, workers rubber-stamped computer printouts without examining them. A Minnesota election official commented: "It's kind of like black magic -- we really don't know what's going on."

3) There are no standards for election software, so anyone can write a vote-counting program. Vendors often talk state legislators into writing enabling legislation which is vague and favors their company. When a state Board of Elections certifies a computer system, the board often fails to consult any computer experts, and when it does consult experts, it may ignore their advice. The state of Pennsylvania certified a computerized election system despite strong objections from two CMU professors. (One of the
~~~~~~~~~~~~~~~~

CMU professors, Michael Shamos, wrote a report called "The Votomatic Election System: An Evaluation" in November 1980.)

4) Vendors consider their software to be proprietary. As a result, in the last 20 years, almost nobody has examined any of the software. Compare this to accounting software, which is subjected to audit by third parties. It is hard to have confidence that software is performing accurately when you cannot look at the code.

Waskell said that states and municipalities have ignored four clear warnings against adopting these systems. In 1970, a Los Angeles blue-ribbon committee recommended that all vote-counting software be independently audited. Similar recommendations have been issued by the National Bureau of Standards (1975), CMU computer science professor Michael Shamos (1980), and the independent auditing firm of Coopers & Lybrand (1982). Nevertheless, none of the programs has been audited.

According to Waskell, vote-counting programs are typically 4,000-5,000 lines of COBOL "spaghetti code." Earlier this year, an Indiana consulting firm analyzed CES's program on behalf of one of the losing candidates who is suing CES. They found numerous problems, including the following:

The translation between the Hollerith punch card code and characters was nonstandard. The 1971 NCR system which the software ran on did not use standard EBCDIC.

The contents of memory were continually being redefined. Numerous variables and fields were overlaid in memory.

The same memory locations were re-used for the vote counts of different races.

There was a total lack of structure. The program contained no PERFORM UNTIL (DO-loop) statements but had numerous undocumented GOTOs.

COBOL's ALTER verb was used, producing self-modifying code.

A call was made to an undocumented, unknown subroutine.

The program interacted heavily with the operator, who can operate the console switches to examine and modify any part of the memory or program after each set of data is tallied.

The program made it easy for the operator to turn off error logging and audit trails, without leaving any trace.

There was heavy use of control cards in the data deck to redefine data fields, raising the possibility that a "knowledgable" voter could punch a control card and drop it into the ballot envelope to change the program's processing of election results.

CES sends undocumented "updates" to election personnel before each election.

The program used a time card to set the time and required that the computer's clock be disabled. This makes it impossible to determine how long the program runs or to accurately determine when logs or printouts are produced.

The program did not correctly count "crossover votes," in which, for example, a voter punches a vote for a straight Democratic ticket and punches votes for several individual Republicans. Before an election in West Virginia, newspaper publicity specifically said that such votes were allowed, yet the program failed to count them.

The program failed to keep a count of invalid ballots.

A report to the Illinois Board of Elections in September, 1985, revealed that of the voting systems that the state tested before elections, 28% contained errors. Although those errors were corrected, such a high error rate suggests that many errors are never detected or corrected. Waskell said that other states' election officials are unaware of the Illinois findings. It disturbed her that Illinois failed to keep a record of the errors it found, but simply sent them back to the vendors for correction.

Suits against CES have been filed in Indiana, West Virginia, and Florida, but judges have dismissed several of the cases for lack of evidence, saying that computer experts' testimony is mere "speculation" and "suspicion." It is hard to successfully prosecute such a case when the computer system itself is designed to ensure that no evidence exists.

In the Indiana case, the plaintiff charged that a CES representative was in the counting room on election night, turned off the program's logging, and added two extra control cards after the last votes were counted. In the West Virginia case, a CES representative allegedly connected a modem to the computer and was down on his hands and knees around the compter on election night, claiming that "a screw was loose." In addition, the West Virginia candidate alleged that the county clerk's husband manipulated the computer's switches during the count. Evidence in this case is difficult to obtain because the county clerk destroyed all the ballots 61 days after the election and returned the program deck to the vendor.

According to Waskell, a company called Cronus recently purchased both CES and two of its competitors, Thornber and Governmental Data. Together, these three companies market 60-80% of the voting systems in use. Cronus is financially tied to the Tyler Corp., whose chief executive officer is Fred Meyer, the Republican Chairman of Dallas County, Texas. Meyer announced his candidacy for Mayor of Dallas one month after the city bought a CES voting system.

Ms. Waskell closed her presentation with a series of recommendations. The Federal Government, using election powers outlined in the constitution, should mandate that all vendors conform to NBS standards. State election laws should be changed to show a greater understanding of the technologies. Local election officials must ensure that audit trails are always turned on and that they are continuous and unbroken. Also, local officials should count a random 5% sample of the vote by a different method, thoroughly test computer systems before adopting them, and be accountable and responsible for their use.

People interested in more information about this subject may want to read New York Times articles by David Burnham, published on 7/29/85, 7/30/85, 8/4/85, 8/21/85, 9/24/85, and 12/18/85, and a letter to the editor, 8/6/85. Ms. Waskell was the source for much of the information in these articles. If you write to me (newman@mit-athena), I can tell you how to reach Ms. Waskell--I'm uncertain whether she wants her address & phone number posted on the net.

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 2: Issue 43

Thursday, 17 Apr 1986

Contents

Re: Review of *Softwar*

Marvin Schaefer <Schaefer@USC-ISI>
15 Apr 1986 09:37-EST

I have read <<Softwar<> only in the French version, and it is interesting to see from Gary Chapman's review that several differences appear to have been worked into the details of the plot to make it more suitable for American [re]viewing audiences.

Of particular note is the agency with which the American hero is associated -- a Langley, Va. organization called NSA (the National *Software* Agency) has been chartered with two primary missions: software debugging and -- software bugging! With only modest chauvinism the authors point out that the French-derived programming language Ada has been chosen as the primary tool for achieving the software debugging mission since it makes it so much easier to locate programming errors. [There are lots of justified paeans to French superiority in software engineering.] Interestingly, the book's NSA does not seem to have any interest in the use of methodological system development techniques in which the intention is to produce correct code in the first place. One is forced to wonder how they intend to produce correctly working softbombs to start with. Perhaps the two directorates do not talk with each other.

The first softbomb is discovered by the soviet computing scientist by analysing a trace of program execution. He correctly finds that the softbomb code executes less frequently than the other instruction sequences in the massive meteorological program, and is thus able to identify its trigger.

Not so the more elaborate examples of hardware subversion that follow in the book's development.

The amount of blind trust that is placed in hardware correctness over that of the software is a realistic assessment of the fairly commonly misplaced faith that one sees today. The attribution to the 'NSA' of the view that using the new high-tech Ada will lead to lower costs and higher reliability (because of cheaper debugging) is an opinion one frequently hears in government.

The book, albeit oversimplified, was fun to read. I found the social implications of the book to be far more interesting than the description of sophisticated computer virus attacks that was mentioned in the Scientific American review a couple of years ago.

Marv Schaefer

GREAT BREAKTHROUGHS [Red Herrings swimming upstream?]

Herb Lin <LIN@MC.LCS.MIT.EDU>
Wed, 16 Apr 86 18:07:03 EST

> From Dave Parnas:
>
> The Fletcher panel... They even rejected a military-like hierarchical command structure for the computers so that there would be no "Achilles Heel" in the system.

And then the Eastport panel went ahead to propose just that!!

> Fossedal's reference to "a single error" is part of another red herring in which SDIO supporters claim that the critics want perfection. The only reference to "error free software" came from SDI supporters, none of the critics have assumed that perfection was needed.

The person who said this was Fletcher himself!

Star Wars software advance

Peter G. Neumann <Neumann@SRI-CSL.ARPA>
Thu 17 Apr 86 17:36:15-PST

Defense Secretary Caspar Weinberger disclosed new scientific advances yesterday that he said provide ``solid reasons'' that a Star Wars anti-missile defense system can be made to work...

Scitech [Princeton NJ, not to be confused with Sytek, of Sunnyvale CA] developed a means for identifying ``rocket plume signatures''... LTV [Dallas] then modified that system to create a special computer program, or algorithym [sic], that can be loaded in the sensors aboard a missile interceptor.

The sensors lock on the plume of fire from an enemy rocket, but the new program makes the necessary corrections to ensure that the intercepting missile hits the enemy rocket and not the plume.

This advance is important because it suggests that enemy missiles can be attacked during their earliest, or boost, stages of flight and are gliding on a trajectory toward earth... [Associated Press, 17 April 86]

[It all reduces to a SMOP
(Small Matter of Programming)!
(See the Hacker's Dictionary.)]

Smart bombs in Libya

Peter G. Neumann <Neumann@SRI-CSL.ARPA>
Thu 17 Apr 86 17:34:28-PST

The U.S. Military now believes that damage to the French Embassy and a residential neighborhood in Tripoli during Monday night's raid on Libya was caused by a Air Force ``smart bomb'' that went astray either because it was dropped by a damaged F-111 jet or because its guiding laser beam was blocked by clouds, Defense Department officials said yesterday...

[The] second explanation is also consistent with the likely trajectory of the bomb, however. The 2000-pound GBU10 bombs ae designed to home in on a beam of light which the ``Pave Tack'' system on the plane's underbelly focuses on the target. After the bomb was dropped, the F-111 probably swerved and climbed to evade anti-aircraft fire, while the laser designator on the undercarriage automatically swiveled to keep the target illuminated. As the plane moved, however, the laser beam may have been broken by smoke or clouds that were drifting over Tripoli Monday night, causing the bomb to fall unguided into the residential neighborhood. (Washington Post, 17 April 86)

Pacific Bell Bills

Peter G. Neumann <Neumann@SRI-CSL.ARPA>
Thu 17 Apr 86 17:36:47-PST

The San Francisco Chronicle of 3 April 86 had this story that I meant to include earlier.

> More than a million California telephone customers will be getting an unpleasant surprise in their April bills because of an equipment malfunction... Because of the goof, these customers were not billed for millions of medium- and long-distance calls since November, said company spokesman Roger Orr. The calls not billed in January and February will show up on the April bill, Orr said. The California Public Utilities Commission

> will not allow the phone company to charge for calls missed by the billing equipment in November and December. Switching machines logged each call but did not put some of them on customers' bills... [No estimate given of how much revenue was lost.]

BU joins the InterNet...

Barry Shein <bzs@bu-cs>
Thu, 17 Apr 86 13:27:24 EST

I may as well tell this anecdote before others do...

Boston University this past week submitted their host table for inclusion in the NIC table. Unfortunately, there were a few entries in the table that should never had made it. The most interesting was a one character nickname ("A") for host BU-CS (local convenience.)

Apparently a bug in the 4.2bsd program htable program which converts from standard NIC format to the format UNIX uses proceeded to fill your disk when it hit this entry. I suspect from the notes that some hosts must pick up the table automatically in the wee hours and do the conversion with a command script so they came in the next morning with a disk full of the string "BUCSA". I was assured by one site that he no longer needs any mnemonics to remember our name. I have no way of knowing numbers, but apparently some number of machines went down or were crippled.

In addition, there was an entry for a machine type "3B2", htable broke on that also although not so dramatically, because the string started with a digit. It seems the next night or so htables were breaking again because someone managed to put a lower case letter into the table. (I have heard this only second hand.)

I then fixed our host table to avoid the troubles and ran it through htable myself just to be sure and it promptly deleted the first entry in my table. Apparently it had to have at least one blank line before the first entry, again, without warning.

This is after almost three years of the program being in production at probably thousands of sites. Don't trust any program over 30 (lines of code)?

-Barry Shein, Boston University

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 2: Issue 44

Monday, 21 Apr 1986

Contents

Why Simulation Is A Good Thing...

<<moorel@eglin-vax> Lynne C. Moore>
0 0 00:00:00 CDT

We are currently engaged in developing a system of remote video tracker pedestals for tracking missile tests, and have recently chosen to implement an interim hardware solution to allow time for a rational software development cycle (rather than 25K+ lines in less than 6 months with 2 programmers). One of the proposed advantages of the software solution is the ability to run a real-time simulation for operator training, and there have been some questions from our top management about why the software developers insist that this is exceptionally important.

Yesterday, an operator attempted to manually track a live missile for the first time. He tracked it for about 1/2 second, and then commented, "Gosh, that thing moves a lot faster than I thought." Too bad none of the managers were there...

Lynne C. Moore <moorel@eglin-vax.arpa>

Hacking & forgery laws

Robert Stroud <robert%cheviot.newcastle.ac.uk@cs.ucl.ac.uk>
Fri, 18 Apr 86 10:18:28 gmt

This was printed in The Times yesterday April 16th. I am particularly intrigued by the prosecution under the forgery laws. I don't see how you can forge something like a telephone number - surely to be protected by a forgery law, an identification should be personal in some sense. Numeric codes are completely impersonal.

===
Prestel blunder 'helped hacker'. (c) Times Newspapers Limited, 1986

A top-level blunder allowed a computer journalist to penetrate British Telecom's Prestel information system, a court was told yesterday. A secret identification code allowing access to secret files was left unprotected within the computer system it was said. Mr Robert Schifreen, aged 22, used it to get the confidential identity numbers and passwords of every Prestel customer, Southwark Crown Court was told.

Mr Schifreen, who subscribed to Prestel under the codename "Bug Hunter", later wrote an article on how easily he had cracked the system. But Mr Schifreen, who works for a computer magazine, denied he did so for personal gain, and accused Prestel of "negligence".

Mr Austin Issard-Davies, for the prosecution, said a random experiment first gave him the telephone numbers of Prestel's private computers. The telephone numbers were not published to normal subscribers, and only a few people had access. But Mr Schifreen was said to have broken into the Prestel development test computer. It was alleged that he typed an experimental line of numbers, all twos, when the computer asked for a 10-digit identification. It worked, and the computer then asked for a four-digit password. He typed 1234 which turned out to be a test account and gave him access. But Mr Schifreen's attempts to get information out failed because he did not have the confidential identity code and password of the system manager. Nine months later, he came across the code and password "lying around" in one of the private Prestel computers.

When questioned by police, Mr Schifreen allegedly admitted making unauthorised access into the system from his home computer, but claimed he had made Prestel more secure by doing so. Mr Issard-Davies said: "It is a bit like a burglar claiming all the credit for improved house security because the householder has put locks on all the windows." He added it was "twentieth century" forgery because Mr Schifreen allegedly used someone else's computer identification, like signing someone's name without consent.
[omitted material]

The charges have been brought under section one of the Forgery and

Counterfeiting Act, 1981. The test case trial is the first contested case
to go to court. The hearing continues today.
==

Robert Stroud,
Computing Laboratory,
University of Newcastle upon Tyne.

ARPA robert%cheviot@ucl-cs.ARPA
UUCP ...!ukc!cheviot!robert

[I reported on a breakin to British Telecom's Prestel Information Service in the ACM Software Engineering Notes vol 10 no 1 (January 1985). A 19-yr-old young man had penetrated the unencrypted password file. To demonstrate the vulnerability, he let a London Daily Mail reporter watch (reported in the LDM on 2 Nov 84) while he read Prince Philip's mailbox and then altered a financial market database. Things seem not to have improved much. PGN]

Strategic Systems Reliability Testing

Dan Ball <ball@mitre.ARPA>
Fri, 18 Apr 86 14:45:03 est

It has been about twenty years since I've worked with strategic systems (Polaris), but I can no longer resist putting in my two cents in the SDI debate.

The issues concerning whether SDI can be made to work perfectly or even well enough the first time since it can't be tested in a realistic environment and there will be no second chance would appear to apply equally to both the US and Soviet Offensive Systems.

During my four years with the Polaris Test Program, I know of no test involving more than a single live missile. Although these tests were for the most part very successful, there was never an attempt to test the ripple fire capability with real missiles on a single submarine, let alone a coordinated launch involving all submarines as well as all land based ICBMs.

In addition to the readiness/reliability considerations of our strategic nuclear forces, I would suspect that the command and control problems would be formidable. We seem to have considerable difficulty sending a single urgent message (e.g. USS Liberty, USS Pueblo, USAF EC-121, etc.) , let alone a coordinated attack involving hundreds or thousands of platforms.

I'm relatively certain that the numbers of warheads actually reaching the target following the initiation of an attack would be far less than the numbers in the inventories.

Finally, the briefing from SDI office that I heard didn't promise perfection. Unlike some of the political supporters who promise that it will be safe for children to play outside during a nuclear exchange, the SDI technical types

were talking about the impact it would have on the numbers and required
modifications to the Soviet ICBMs that would be required for them to
maintain the same confidence of assured first strike destruction of the US.

(I promise that this will be my first and last comment concerning SDI as I
think there's far too much uninformed speculation and political opinion on
this subject in risk-forum already. I'll even volunteer to be edited out as
I would like to see more contributions that could help those of us whose job
is trying to assure that computer reliability and safety requirements are met.)

Dan Ball

[Don't bet on there being no provoking replies. PGN]

SDI

<decvax!bellcore!genrad!panda!talcott!maynard!campbell@ucbvax.berkeley.edu>
Fri, 18 Apr 86 07:19:30 EST

The discussion in the last few issues of RISKS has demonstrated that Reagan's
Strategic Defense Initiative HAS ALREADY SUCCEEDED. It has done exactly
what Reagan wanted, which is to convert an essentially political question,
in which every American is qualifed and in fact obligated to participate,
into a technical debate, in which only the technical clergy are allowed.

Larry Campbell The Boston Software Works, Inc.
ARPA: maynard.UUCP:campbell@harvard.ARPA 120 Fulton Street
UUCP: {harvard,cbosgd}!wjh12!maynard!campbell Boston MA 02109

Cost of phone billing error

David Redell <redell@src.DEC.COM>
Fri, 18 Apr 86 09:50:03 pst

> More than a million California telephone customers will be getting an
> unpleasant surprise in their April bills because of an equipment
> malfunction...[No estimate given of how much revenue was lost.]

The estimate I saw was $25-30 million.

Normal Accidents and battle software

Dave Benson <benson%wsu.csnet@CSNET-RELAY.ARPA>
Sun, 20 Apr 86 21:51:10 pst

According to

Charles Perrow
Normal Accidents: Living with High-Risk Technologies

Basic Books, New York, 1984

we should expect to see large-scale accidents such as the loss of the space shuttle Challenger. Perrow's thesis, I take it, is that the complexity of current technology makes accidents a 'normal' aspect of the products of these technologies.

We may view space shuttles launches, nuclear reactors, power grids, transportation systems, and much real-time control software as lacking homeostatis, "give", forgiveness. Perhaps some of these technologies will forever remain "brittle".

Questions: Does anybody have a good way to characterize this brittleness? To what extent is existing battle software "brittle"?

Thank you for your suggestions/comments   dbb

Psychological risks, part II

Dave Benson <benson%wsu.csnet@CSNET-RELAY.ARPA>
Sun, 20 Apr 86 21:59:17 pst

I have just finished reading

Neil Frude
The Intimate Machine
New American Library, New York, 1983

which comments on animism and anthropomorphism in the past and present, and speculates on the continuence of these tendencies into the future with human-like qualities in computers.

I did not find the argument persuasive, but then I bang at this terminal quite a bit, and certainly do not anthropomorphize it in the slightest.

Perhaps some of you have <modern> stories about people who view computers as having human-like qualities, confusing their perceptions of humans and computers. If so, please send such direct to me unless you think them generally enlightening RISKS. Thanks, dbb

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 2: Issue 45

Monday, 28 Apr 1986

Contents

HBO gets Hacked:: We Interrupt This Program ... for a Viewer Protest.

the tty of Geoffrey S. Goodfellow <Geoff@SRI-CSL.ARPA>
27 Apr 1986 15:51-PDT

NEW YORK (AP) - A video hacker calling himself ''Captain Midnight'' startled cable television viewers from Maine to the Plains early Sunday when he interrupted a movie on Home Box Office with a printed message protesting HBO's scrambling of its satellite-to-earth TV signals.

''It's a criminal, willful interference of a government-licensed satellite broadcast,'' fumed David Pritchard, an HBO vice president, who said the cable system had received sabotage threats in recent months.

Pritchard said HBO planned to report the incident to the Federal

Communications Commission.

''It's kind of like terrorism of the airwaves,'' said Greg Mahany, who was watching in Middletown, Ohio, when the message interrupted ''The Falcon and The Snowman.''

The message, printed in white letters on a color-bar test pattern background, read: ''Goodevening HBO from Captain Midnight. $12.95 a month? No way! (Showtime-Movie Channel Beware.)''

Mahany said that at first the picture flipped back and forth between the message and the movie, making it seem like ''HBO was trying to get its signal back. ... It looked like a fight for control of the microwave beam.''

The message appeared at 12:30 a.m., Eastern time, and remained on the air about five minutes. It was seen in the eastern two-thirds of the nation, which accounts for more than half of HBO's 14.6 million subscribing households.

Pritchard said the hacker, apparently with the use of a satellite dish and a powerful transmitter, effectively replaced HBO's signal with his own.

For some reason - possibly because Captain Midnight's signal was better-timed or more powerful - HBO's satellite received the hacker's signal instead of HBO's and beamed it down to HBO's earth relay stations.

Sunday's intrusion was immediately noticed at HBO's communications center in Hauppauge, N.Y., but it was not clear whether the hacker ended his own message or was forced off by HBO.

Pritchard said HBO would have no comment on that. ''We have implemented some technical remedies, and we're pursuing others,'' he said. ''This represents a clear danger to every satellite user.''

Pritchard said action like Sunday morning's had been threatened in letters to HBO and in magazines read by dish owners.

''We'd been threatened for the last four or five months with something like this if we didn't reconsider our plan to scramble,'' he said. ''They said they'd do something. They didn't say what.''

The HBO cable signal is scrambled to prevent reception in homes wired for cable television but not equipped with an HBO converter. Until earlier this year, satellite dish owners were able to intercept the unscrambled signal HBO bounces off satellites to the earth stations that relay the signal via cable.

In January, however, HBO began scrambling all its satellite-to-earth signals. HBO told dish owners who had been watching for free they would have to buy a descrambler for $395 and pay $12.95 a month.

Another leading pay cable service, Showtime, announced plans for a similar system.

Pritchard said about 6,000 dish owners put down the cash for the decoder and signed up for HBO or its sister service, Cinemax. But the proposal has been unpopular with others.

''They say things like, 'The airwaves are free,' and 'They (HBO) are using government satellites that our taxes pay for,''' Pritchard said.

Pritchard said HBO's programs are its property, and it leases space from privately owned satellites.

HBO gets Hacked:: We Interrupt This Program ... for a Viewer Protest.

"Frank J. Wancho" <WANCHO@SIMTEL20.ARPA>
Sun, 27 Apr 1986 22:39 MDT

> Until earlier this year, satellite dish owners were able to intercept the unscrambled signal HBO bounces off satellites to the earth stations that relay the signal via cable.

It is interesting to note that while protective "alledgedly" and similar words are freely sprinkled in newsprint, the writer of the above chose "intercept" over "receive". The word "intercept" implies "theft", a criminal act. That "intercept" was unmodified and not a quote implies the allegation was accepted as fact proven in court. Is this indeed the case, or simply the viewpoint held by the programming services? If the latter, then it was inappropriate and perhaps biased to use "intercept".

Just asking...

--Frank

Ball's contribution on Polaris and SDI (from Dave Parnas)

<Neumann@SRI-CSL.ARPA>
Tue, 22 Apr 86 07:37:13 pst

Dave Parnas is now on his way to Australia for almost two months, so please don't expect him to reply. But on his way out, he sent me this (which I include with his permission):

> As I read the first part of Ball's contribution, I was sure he was agreeing with me, but no, as I read on I saw that he was on the SDIO side. His arguments are simple and they are the arguments that the other defenders of the program make.
>
> (1) The weapon systems that we have now have not been adequately tested and probably won't prove reliable so we can build another one with those properties. It's "business as usual".
>
> (2) Its quite alright to allow the President, the Coalition for Star Wars, and High Frontiers to tell the public and congress that they are "making nuclear weapons impotent and obsolete" , "ending the fear of nuclear weapons" and trying to end the "immoral" policy of deterrence, while using those funds to do something quite different. Misrepresentation is "business as usual".
>
> His message reconfirms my assertion that there is no doubt about the technical facts. We cannot build a system that does what the president asked us to do and what the supporting public wants. Almost nobody working on it believes we can. Its not a question of perfection. It is a question of effectiveness and reliability. The reliability of such a system will always be in question; its effectiveness will always be unknown. We

will always know that there are effective countermeasures. It will not lead
to increased security. It will lead to "business as usual".

Dave

SDI Reliability Testing - Offensive deterrent vs SDI

Jon Jacky <jon@uw-june.arpa>
Mon, 28 Apr 86 00:13:10 PDT

> (Dan Ball writes)
> The issues concerning whether SDI can be made to work perfectly or even
> well enough the first time since it can't be tested in a realistic
> environment and there would be no second chance would appear to apply
> equally well to both the US and Soviet offensive systems.
>
> During my four years with the Polaris Test Program, I know of no test
> involving more than a single live missile ... I'm relatively certain that
> the numbers of warheads actually reaching the target following the
> initiation of an attack would be far less than the numbers in the
> inventories. ... In addition ... I would expect that the command and
> control problems would be formidable.

This point is well taken. Still, I think there are two important differences in degree, if not in principle:

1. To have the desired deterrent effect, at least given today's very large arsenals, it is not necessary that most weapons work especially well. It is only necessary to create the impression that something pretty awful would happen if we attempted to use some of them.

2. The coupling between each weapon and other systems appears to be weak. In particular, it is my understanding that once a missile is fired, it is entirely self-guided, and does not depend on the correct functioning of any other systems. This is in contrast with your typical SDI scheme, which depicts a ground based laser bouncing its beam off two aiming mirrors on opposite sides of the planet, with various observation and battle-management satellites hovering nearby. Without this being an explicit design goal, the present offensive system seems to have achieved the desirable quality of having a "system behavior which can be inferred from its components" in the Eastport panel's words.

My point is that testing a missile defense system is a much tougher job than testing the offensive system it is supposed to defeat, if an equivalent level of confidence is desired.

Note that this is true only if the offensive missile system is for deterrence. If it is supposed to carry out a first strike, or any other highly-coordinated activity - "counterforce," "countervailing response" or whatever you call it -- the difficulty of obtaining confidence in the offensive system becomes much greater. There is a huge literature of analysis and simulation devoted to highly coordinated offensive attacks. I have no idea whether

policy makers regard these at all seriously, but I think it is
important for technical people to point out that very little of this
has been tested in realistic conditions and it is anybody's guess what would
happen if anyone actually tried to carry out such plans.

> The briefing from SDI office that I heard didn't promise perfection ...
> I think there's far too much uninformed speculation and political opinion
> on this subject in risks-forum already ...

People hear various things from people associated with SDI. As far as I know, there is still no official statement of what SDI's performance requirements are. Until there is, discussion is necessarily limited to speculation and generalities. What is required, of course, is some quantitative requirement such as, "The defense must stop at least 90% of an attack by 1000 ICBM's," or "The defense must preserve at least 50% of our land-based missile silos." Then, we could discuss what tests, if any, could make us confident that the requirements would be met in a real attack. Discussion of whether the requirements were consistent with earlier promises to render missiles impotent, etc., do include political opinion and could be forbidden by the editor.

-Jonathan Jacky
University of Washington

What are the limits to simulation?

Eugene Miya <eugene@AMES-NAS.ARPA>
23 Apr 1986 1518-PST (Wednesday)

> Subject: Why Simulation Is A Good Thing...
> From: Lynne C. Moore
>   Description of a tracking system.

The Subject field described is certainly well intended, but I really wonder what simulation's various limits are. Simulation is really only an extension of human intellect, not the way things behave in Nature. While I do not take issue that some simulation is a good thing, I wonder where this ends? What are limits: first social, next might be performance related. I think there has been an penchant towards things like simulation and non-destructive testing, etc. of late, but we have recently seen with the Challenger incident, that our best laid plans run into problems. I wonder if we have not taken these techniques, too far? Perhaps we have to keep extra margins for error and destructive testing (however expensive) in tact. Consider:

Would YOU step into a plane which has only been simulated and never test flown?

Consider that chemistry classes uses dangerous chemicals, should we or should we not replace such chemicals with computers and `simulate' reactions? An educational point.

Would you trust YOUR life to a system like MYCIN? Suppose I infected you with a disease like Anthrax, and said, identify it. [Note the US Army did and does infect volunteers with various fatal diseases to test vaccines and treatments.]

I've had people say, after seeing the first computer graphics planetary flybys: "Hey that's really neat! Why send expensive spacecraft up there when you can generate simulations like this?"

Do computer scientists sometimes have difficulty in distinguishing "reality?"

While it is true that computers can and will do somethings better than humans, I wonder where and how we will describe that limits. What about dissent?

I think the people with the greatest humility (and perspective)
in simulation are the physicists who do weather prediction and analysis.
[Note early simulations took 27 hours to run a 24 hour forecast.]
Nothing like running a weather code, then looking out the window.

--eugene miya

Reference on admissibility of computer records

Bill Cox <bill@crys.wisc.edu>
Wed, 23 Apr 86 00:50:40 CST

This is a copy of an article submitted to mod.legal on usenet.

Subject: Re: Admissabilty of computer files as evidence
Newsgroups: mod.legal
To: info-law@sri-csl.arpa
Summary: article in ACM TOOIS on admissibility of computer-generated records
References: <8604171858.AA03202@taurus>

There is an article in ACM TOCS that has some relevance to the subject.

> Roger King and Carolyn Stanley, "Ensuring the Court Admissibility of Computer-Generated Records", ACM Transactions on Office Information Systems, Vol 3, Number 4, pp398-412.

The focus is on issues related to accounting records, e.g., "What does Smith owe my company", but also discusses issues in conspiracy cases where "computer-generated records to prove essential elements of [the government's] case."

There are relevant legal citations, and references to the Federal Rules of Evidence and their current application to computer-generated records.

I think this article is in the "must-read" category for anyone interested in both law and computers. I am a novice in the law [I've paid many dollars to attorneys, and a little of the knowledge rubbed off], but I must say that this article seems well-researched and quite thorough.

William Cox
Computer Sciences Department
University of Wisconsin, Madison WI
bill@wisc.crys.edu
...{ihnp4,seismo,allegra}!uwvax!bill

Phone billing error at Pacific Bell, etc.

John Coughlin <John_Coughlin%CARLETON.BITNET@WISCVM.WISC.EDU>
23 Apr 86 00:11:19 EST

> More than a million California telephone customers will be getting an
> unpleasant surprise in their April bills because of an equipment
> malfunction...No estimate given of how much revenue was lost.|

According to Computer Chronicles on PBS tonight the "reprogramming error" cost Pacific Bell $51 million. In a related story, students in Arkansas obtained a confidential telephone number from Southwestern Bell's computer system which enabled them to place thousands of free long distance calls. Also, a long lineup at a particular pay phone in a Sears store in Hackensack tipped off police to the fact that one could use it to place international calls free of charge. Apparently 400 phones were affected by this software bug.

/jc

Unconfirmed information tells that the US-attacks on Libya on 24 March and 15 April were possible due to outmaneuver of the libyan air defense system which is russia-provided. USS Caron and Yorktown were illegally crossing the 12-mile line in front of the military harbor Sewastopol in the Black Sea on 13 March 86. They alerted the russian defense system and collected all relevant electronic data. (Some sources say that the Korean Jumbo which was shut down over Sachalin in 1983 also was alerting the defense system, and a satellite recorded the signals.) Knowing the signals the US were able to circumvent the air defense system and get into the country without loss. Now Gaddafi is not willing to pay Russia for the system. And Russia needs to update its system for many millions.

What if espionage of the western defense system and circumvention is as simple and possible??

Udo Voges idt766%dkakfk3.bitnet@wiscvm.arpa

Challenger article

<Rminnich@dewey.udel.EDU>
Fri, 25 Apr 86 12:03:25 EST

The following article appeared in the Phila. Inquirer of 4/24.

Since the Challenger was discussed on Risks by people in the know, I wondered if we could hear some more opinions. The writer is William V. Shannon, with the Boston Globe.

I am excerpting; it is a long article.

"... It is now clear that there was no explosion ..."

"... The astronauts ... were probably making frantic efforts to bring their craft under control as it hurtled downward. If the craft had been equipped, as it should have been, with parachutes and seat-ejection fail-safe systems they could have saved themselves. "

"They died because of NASA's false economies and incompetence. "

"... Dr. William Doering, professor of chemistry at Harvard, pointed out that ... was not an explosion at all. 'It is best described as a fast fire ... If the fuel tank had exploded ... it would be producing something much bigger ... They have stopped showing the space module [sic] but I am confident that it is intact also or was until it hit the water. '"

"... Terry J. Armentrout, director of the NTSB investigation, told reporters that '... the shuttle Challenger, including the crew compartment, apparently survived the blast mostly intact'".

Continues Shannon,

" ... the astronauts died from the force of the impact as the craft hit the water ... There is no reason to believe that the crew died because of sudden decompression ..."

He goes on to hint that the down-link was lost as part of a cover-up rather than due to the fast fire.

OK. I do not know if the Moderator wants to see replies or comments about this on RISKS; if not, please send me any thoughts you might have. I will send them on to the paper. Maybe this guy is absolutely right, but I have my own thoughts on that.

ron minnich

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 2: Issue 46

Tuesday, 29 Apr 1986

Contents

Re: Challenger article

<mooremj@eglin-vax>
0 0 00:00:00 CDT

> From: Rminnich@dewey.udel.EDU
> [excerpts from article Phila. Inquirer of 4/24.]

>   "... It is now clear that there was no explosion ..."

Rubbish. There was certainly an explosion; what do they think scattered debris for miles and threw some so high it took an hour to impact? That it was not an all-consuming explosion as was originally thought, is now obvious. But I still wouldn't want to be anywhere around an explosion like the one we saw.

>   "... The astronauts ... were probably making frantic efforts
> to bring their craft under control as it hurtled downward. If the
> craft had been equipped, as it should have been, with parachutes and
> seat-ejection fail-safe systems they could have saved themselves. "

According to figures I have seen in the news media (AP stories, I think;

the newspapers are in the trashpile now) at the moment of downlink loss the cabin pressure was 800 psi and the acceleration was 16g. These were extrapolated to be 2000 psi and 100g a few seconds later. These are obviously unsurvivable in themselves, not to mention that the cabin windows would not have survived the overpressure, resulting in explosive decompression, which is not exactly healthy either.

Of course, *if* anyone survived the initial blast and remained conscious, I'm sure they would have made frantic efforts to bring the craft under control (who wouldn't?). On the subject of parachutes, I think that any external parachute system would certainly have been burned away or ripped away by the initial blast. As for ejection seats, these may or may not be useful; I believe there are severe technical problems (I'll have to pass on the details -- maybe an expert on the subject will speak up.)

> "They died because of NASA's false economies and incompetence. "

The commission hasn't even made its report yet, but this reporter obviously has all the facts and has completed the inquest. It's true that NASA looks less than pure based on what the media have reported, but this verges on deliberate slander (can you slander a government agency? sorry, I digress.) (Also, let's please *not* start the "whose fault was it" flamage here; those of you who read SPACE are probably more than sick of it by now, as I am.)

> "... Dr. William Doering, professor of chemistry at Harvard, pointed
> out that ... was not an explosion at all. 'It is best described
> as a fast fire ... If the fuel tank had exploded ... it would be
> producing something much bigger ... They have stopped showing the
> space module [sic] but I am confident that it is intact also or
> was until it hit the water. '"

I haven't the chemistry knowledge to dispute this on technical grounds; however, my point about debris scattering still holds. Also, why did he wait until the crew module was found? Why didn't he say after seeing the pictures, "That's not an explosion, it's just a fast fire." Also, what is "intact"? "More or less in one piece" or "completely sound"? Apparently at least the former was true. But the 100g acceleration would pretty well rule out the latter.

> "... Terry J. Armentrout, director of the NTSB investigation,
> told reporters that '... the shuttle Challenger, including the crew
> compartment, apparently survived the blast mostly intact'".

Aw, c'mon! The crew module stayed in one piece, but it was completely separated from the rest of the Orbiter, which was wrecked (it's no surprise that the crew module could maintain its integrity even if no other part of the Orbiter did; it's the strongest part of the Orbiter.)
If the rest of the Orbiter survived "mostly intact" where did the bits of Orbiter wreckage shown by the media (e.g., wing and stabilizer pieces, tiles, etc.) come from?

> Continues Shannon,
> " ... the astronauts died from the force of the impact as the
> craft hit the water ... There is no reason to believe that the crew died

>   because of sudden decompression ..."

Well, they probably died from 100g acceleration before they had a chance to
die from decompression; if not, decompression probably would have done it.
Maybe we'll never know for sure, but I believe the crew died within seconds of
the blast.

>   He goes on to hint that the down-link was lost as part of a
\>cover-up rather than due to the fast fire.

This is so unbelievable that I don't even know what to say. I don't suppose
he offers the least bit of proof? (Speaking from personal experience,
which includes over 100 space launches including the first 8 shuttles,
I would say that there is *no* way such a coverup could be maintained for
long, given the large number of people involved in the launch process.)

As always, I express herein only my own personal opinions, and not the
official position of my employer or any government agency.

Martin J. Moore
mooremj@eglin-vax.arpa

TV "piracy"

<Nicholas.Spies@GANDALF.CS.CMU.EDU>
28 Apr 1986 19:48-EST

The recent "Captain Midnight" episode was, in my book, a completely justified display of civil disobedience. I live in Pittsburgh, which has a (pathetic) cable company to which I subscribe, so I am not an aggrieved dish owner, but I sympathize with them. Why? Because cable program providers MUST factor in ONLY wired-in subscribers when signing contracts to buy programming (or else they are idiots) so the fringe viewers with discs (most often far from any cable company) have little or nothing to do with their financial situations. HBO's decision to scramble its signal to force people who cost HBO, or cable systems, ABSOLUTELY NOTHING to "hook up" is ridiculous; at least disc owners should be given a hefty credit for their investment before having to buy a descrambler and pay monthly rates. Not being a lawyer, it also seems that scambling makes a mockery of the 1934 Communications Act, which prevents encoded transmissions over public channels.

This sort of problem may prevent another medium -- videodiscs -- from fulfilling their promise of providing vast aounts of cheap information. Consider: a 12" videodisc can store up to 108,000 frames of information. What information? In the case of NASA, lots of planetary images. In the case of the National Gallery of Art, 1645 art works and a couple of movies. But what if a videodisc publisher wanted to provide a comprehensive collection of ALL major works of western art, 65 TIMES the number of art works provides on the NGA disc. As it stands, this would be impossible because each provider of art images would want a royalty for each disk (to pay costs, perhaps 1 cent per work per copy. But this would mean a $10,800 royalty PER

DISC for all suppliers, which would make the disc completely unsalable, making a comprehensive history of art expert system all but impossible to develop because the costs could not be amortized. (If you think this is outlandish, consider that the Metropolitan Museum in New York wanted to charge the US Marine Corps $50 for the LOAN of a photograph of an artifact that the Marines wanted to include in their Bicentennial exhibit in Washington DC in 1976. The Marines, to their credit, declined to pay.)

Some new paradigm will have to be worked out before mega-media will be acceptable both to information providers and consumers.

Nick

HBO -- Hacked Briefly Overnight

Mike McLaughlin <mikemcl@nrl-csr>
Mon, 28 Apr 86 21:51:15 edt

Overpowering a transmitter is essentially trivial. If HBO was scrambling its uplink, Captain Midnight's missive must have been similarly scrambled. Perhaps HBO's scramble algorithm is also trivial. Of course, if the uplink is in the clear, Captain Midnight merely needed brute force. Anyone know how or where the signal is scrambled? Or whether an HBO receiver set to unscramble will pass an in-the-clear signal? I realize that facts may set limits to the discussion. Regrettable.

The dangers of assuming too much

<Holbrook.OsbuSouth@Xerox.COM>
29 Apr 86 14:32:33 PDT (Tuesday)

[From "Three Mile Island: Thirty Minutes to Meltdown" by Daniel Ford; Viking Press 1982.]

(The discussion preceeding this quote talks about how the temperature of the fuel rod at Three Mile Island-2 increased from the normal 600 degrees to over 4000 degrees during the 1979 accident, partially destroying the fuel rods. It also notes that instruments to measure core temperatures were not standard equipment in reactors.)

> "Purely by chance, there were some thermocouples -- temperature-measuring devices -- present in the TMI-2 reactor when the accident occured. Located about 12 inches above the top of the core, these thermocouples ... were installed as part of an experimental study of core performance, and were a temporary instrumentation feature of the plant, connected to the control-room computer for measuring temperatures during normal operation. Accordingly, if a control-room operator requested temperature data from the computer, he would receive useful information only when the temperature was within the normal 600 degree range. When the temperature got above 700 degrees, the computer, instead of reporting it, would simply print out a string of question marks -- "???????." Although the thermocouples could

actually measure much higher temperatures, the computer was not programmed to pass these higher temperature readings on to the operators ... there was an urgent need for timely, reliable data about the temperature in the core in the critical period between 6am and 7am on March 28; what was available from the computer was mostly question marks."

Paul

A POST Script on Nuclear Power

Peter G. Neumann <Neumann@SRI-CSL.ARPA>
Tue 29 Apr 86 22:42:21-PDT

While we are on nuclear power plants, please let me know if anyone gets some solid facts that involve the computer-control system in the Chernobyl nuclear accident in the Soviet Union over the weekend ("partial meltdown", "graphite explosion", or whatever it was).

By the way, today's Washington Post gave a chronology of some of the more interesting previous nuclear-power accidents, which I summarize here:

Dec 2 1952 Chalk River, Canada. Million gals radioactive water built up.
  6 mos to clean up. Human error.
Nov 1955 EBR-1 experimental breeder, Idaho Falls. Mishapen rods, human err.
Oct 7-10 1957 Windscale Pile #1. English coast of Irish Sea. Largest
  known release of radioactive gases (20,000 curies of iodine). Fire.
  .5 M gals milk destroyed. Plant permanently shut down.
Winter 1957-58 Kyshtym USSR. 400 mi contaminated? Cities removed from maps.
May 23 1958 Chalk River again. Defective rod overheated during removal.
  Another long clean-up.
Jul 24 1959 Santa Susana CA, 12 of 43 fuel elements melted. Contained.
Jan 3 1961 SL-1 Idaho Falls (military, experimental). Fuel rods mistakenly
  removed. 3 killed.
Oct 5 1966 Enrico Fermi, Michigan. Malfunction melted part of core.
  Contained. Plant closed in 1972.
Jun 5 1970 Dresden II, Morris Illinois. Meter gave false signal. Iodine
  at 100x permissible. Contained.
Nov 19 1971 Monticello Minn. 50,000 gals radioactive waste spilled into
  Mississippi River, some into St Paul water supply.
Mar 22 1975 Brown's Ferry, Decatur Alabama. Insulation caught fire,
  disabled safety equipment. $150 M cleanup.
Mar 28 1979 Three Mile Island II. NRC said, "within an hour of
  catastrophic meltdown". 4 equipment malfunctions plus human errors
  plus inadequate control monitors.
Feb 11 1981 Sequoyah I, Tennessee. 8 workers contaminated, 110,000 gals
  radioactive coolant leaked.
Jan 25 1982 Ginna plant, Rochester NY. Steam-generator tube ruptured.
Feb 22 & 25 1983 Salem I NJ. Auto shutdown system failed twice. Manual OK.
Apr 19 1984 Sequoyah I again. Contained.
Jun 9 1985 Davis-Besse, Oak Harbor, Ohio. 16 pieces of equipment failed,
  at least one wrong button pushed. Auxiliary pumps saved the day.

PGN (just off the plane from DC)

PS. I hope you don't conclude that I am interested ONLY in catastrophes. I really have been professionally involved for many years in trying to develop better computer systems. But that does not mean that I have to trust them...

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 2: Issue 47

Thursday, 1 May 1986

Contents

HBO hacking

Phil R. Karn <karn@mouton.bellcore.com>
Wed, 30 Apr 86 17:58:40 edt

Satellite transponders used by the cable TV industry to relay programs are "bent pipes", that is, they simply repeat whatever they hear. The M/A-Com scrambler equipment is all on the ground. However, the descramblers will switch to "pass through" mode if a nonscrambled signal is received. Therefore, when Captain Midnite sent his unencoded signal, the descramblers simply passed the signal straight through to the various cable systems.

The transmitter power available on a satellite is very limited (5-10 watts). Even with a very large receiver dish, the raw carrier-to-noise ratio is far too low for acceptable picture quality if a linear modulation scheme (such as VSB AM, used for ordinary TV broadcasting) were used. Therefore, satellite TV transmissions are instead sent as wideband FM in a 40 MHz bandwidth. Since the baseband video signal is only 5 MHz wide, this results in a fairly large "FM improvement ratio" and a pronounced "capture" effect. Full receiver capture occurs at about a 10 dB S/N ratio, and this figure is essentially the same whether the "noise" is in fact thermal noise or another uplink signal. So for the purposes of fully overriding another uplink your signal must be about 10 dB stronger (10 times the power).

The latest transponders are much more sensitive than those on the earliest C-band domestic satellites launched 12 years ago. Most of the 6 Ghz High Power Amplifiers (HPAs) in use at uplink stations are therefore capable of several kilowatts of RF output, but are actually operated at only several hundred watts. So Captain Midnite could have easily captured the HBO uplink if he had access to a "standard" uplink station (capable of several kilowatts into a 10 meter dish) or equivalent.

I happened to turn on HBO in my Dayton, Ohio hotel room at about 1AM, half an hour after the incident occurred, and noticed lots of "sparklies" (FM noise) in the picture. At the time I grumbled something about having to pay $90/night for a hotel that couldn't even keep their dish pointed at the satellite, but I now suspect that the pirate was still on the air but that HBO had responded by cranking up the wick on their own transmitter. Because they were unable to run 10 dB above the pirate's power level, they were unable to fully recapture the transponder, hence the sparklies. (Can anyone else confirm seeing this, proving that my hotel wasn't in fact at fault?)

Even though each transponder has a bandwidth of 40 MHz, it is separated by only 20 MHz from its neighbors. Alternating RF polarization is used to reduce "crosstalk" below the FM capture level. Polarization "diversity" isn't perfect, though, so it is possible in such a "power war" that the adjacent transponders could be interfered with, requiring *their* uplinks to compensate, which would in turn require *their* neighbors to do the same, and so on. So Captain Midnite could cause quite a bit of trouble for all the users of the satellite, not just HBO.

Captain Midnite could have been anywhere within the Continental US, Southern Canada, Northern Mexico, the Gulf of Mexico, etc. In the worst case, it could be practically impossible to locate him. If he is caught, it will be either because he shoots off his mouth, arouses suspicion among his neighbors (or fellow workers, if a commercial uplink station), or transmits something (distinctive character generator fonts, etc) that gives him away. Only the NSA spooksats would be capable of locating him from his transmissions alone, and I suspect even they would require much on-air time to pinpoint the location accurately enough to begin an aerial search.

Phil Karn

HBO hacking

Dan Franklin <dan@bbn-prophet.arpa>
Wed, 30 Apr 86 18:11:02 EDT

Re the interception of HBO's uplink by "Captain Midnight": I understand that the video scrambling is indeed pretty simple, consisting of reversing black and white on some "randomly-chosen" scan lines. It's easy to build a box that will undo this scrambling. The sound is much harder; it uses DES. In the accounts I read, Captain Midnight just put up a still video picture with no sound, which would make sense assuming that the uplink is encoded; he could easily encode his video but not his sound.

Nicholas Spies seems to feel that the scrambling was purely an act of malice against individuals with dishes. Not so; according to a recent issue of Forbes, when HBO started scrambling, a number of CABLE TV OPERATORS they'd never heard of signed up for the decoders! If cable TV operators can charge their customers for HBO, why should they get it for free?

I had some other comments about what the FCC Communications Act really says and what "public" means, but this is getting awfully far from Risks... "Telecom" and "poli-sci" are no doubt more appropriate.

Dan Franklin (dan@bbn.com)

[Thanks for the restraint. However, the relevance of the HBO case to RISKS is clear. Various risks exist -- but have been customarily ignored: easy free reception and spoofing without scrambling, video spoofing and denial of service even with scrambling. PGN]

What are the limits to simulation?

Herb Lin <LIN@MC.LCS.MIT.EDU>
Thu, 1 May 86 10:43:02 EDT

From: eugene at AMES-NAS.ARPA (Eugene Miya)

I really wonder what simulation's various limits are.

I believe it was Eddington that said "The Universe is not only stranger than we imagine, but it is stranger than we can imagine."

Strategic Systems Reliability Testing

Herb Lin <LIN@MC.LCS.MIT.EDU>
Thu, 1 May 86 10:41:18 EDT

From: ball at mitre.ARPA (Dan Ball)

I'm relatively certain that the numbers of warheads actually reaching the target following the initiation of an attack would be far less than the numbers in the inventories.

Probably true, if what you mean by target is a hardened silo. But if you aim at the center of a city, and you miss by a mile, that's still "reaching the target" too. And THAT is what the SDI is supposed to protect us against.

Finally, the briefing from SDI office that I heard didn't promise perfection. Unlike some of the political supporters who promise that it will be safe for children to play outside during a nuclear exchange, the SDI technical types were talking about the impact it would have on the numbers and required modifications to the Soviet

ICBMs that would be required for them to maintain the same confidence
of assured first strike destruction of the US.

None of the technical supporters believe in near-perfect defense. But
the political supporters do, and they are lying to the public.

Correction on Challenger Discussion (RISKS-2.46)

Jeff Siegal <JBS%DEEP-THOUGHT@EDDIE.MIT.EDU>
Thu 1 May 86 18:15:43-EDT

> "... Dr. William Doering, professor of chemistry at Harvard, pointed
> out that ... was not an explosion at all. 'It is best described
> as a fast fire ... If the fuel tank had exploded ... it would be
> producing something much bigger ... "

[...] Also, why did he
wait until the crew module was found? Why didn't he say after seeing the
pictures, "That's not an explosion, it's just a fast fire."

It is stated in the original column that Dr. Doering's observation
was made when he watched the videotape, not months later, as Mr.
Moore claims.

Jeff Siegal

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 2: Issue 48

Saturday, 3 May 1986

Contents

Failure to Backup Data

James H. Coombs <JAZBO%BROWNVM.BITNET@WISCVM.WISC.EDU>
Fri, 2 May 1986 20:22 EDT

Experienced computer users are aware that they must backup their data regularly to ensure that the inevitable hardware/software failures and operator errors do not cost them months of work and considerable stress. In most mainframe environments, users are supported by well-designed backup systems--including off site storage of tapes. With the first wave of microcomputers, people found that facilities for backing up their work were inadequate: they consume too much time and are hard to organize. Consequently, few microcomputer users can recover all of their work up to the previous 24 hours. The majority of users would lose years of work if the site were destroyed or seriously damaged. In fact, most people consider themselves "lucky" if they can recover even a small portion of their work. [I should add that I know of one heavily-used VAX that gets backed up quarterly at best.]

Unfortunately, we are in the process of introducing more and more professionals to computers. We tell them that their work will be faster, more efficient, and possibly even better. From a recent survey of my department (English), I would estimate that about 90% of "them" believe us. So, we are about to equip these people with workstations and will teach them to develop their books on these machines. Unfortunately, no one has mentioned backup at all so far, in spite of the fact that these machines are rumored to eat files and directories. Even if we assume that professors will be admonished to backup their files regularly, we cannot be so naive as to assume that they will if it takes more than a few minutes. Since a complete backup of a 10 megabyte hard disk on an IBM XT can take a half-hour, I am sure that backing up a 40 megabyte hard disk on a workstation will require more time (and diskettes) than the majority of our scholars will invest. Now, one of these people is going to lose a book, or most of a book. And s/he is not going to be happy. In fact, I think we can be sure that new users will not ever want to see a computer again, and colleagues may be scared off as well. In addition, someone is going to be held accountable.

Here is a brief tally of the risks:

1) loss of work by the professor

2) loss of interest in computing by the professor and some colleagues

3) loss of confidence in departmental consultant (me)

4) loss of confidence in project team heading the project

There may be others, and (1) may actually be much more severe than a loss of work. A delay of a couple of months in developing a manuscript could cost a young professor tenure, for example (assuming that given the seasonal nature of academia, a two month delay in submission could cause a six month delay in acceptance or could make one's work obsolete because of another publication).

I would like to hear from others who have faced these problems. Horror stories, preventive strategies, references to theoretical articles--all would be useful. I suppose that there may be legal considerations as well?

--Jim Coombs, Brown University
            JAZBO@BROWNVM
Acknowledge-To: <JAZBO@BROWNVM>

Computer detracting from effective communication?

<rti-sel!dg_rtp!rtp41!dg_rama!bruces%mcnc.csnet@CSNET-RELAY.ARPA>
Fri, 2 May 86 20:13:18 edt

ARE WORD-PROCESSING AND ELECTRONIC MAIL HELPING TO PROLIFERATE BAD WRITING?

Before word processors and electronic mail existed, important letters or documents were usually handwritten and hand-corrected, often in several drafts, before being typed and mailed. The typing of the letter represented a finalizing and codifying process which encouraged well thought-out communication. Care needed to be taken, since a single error could necessitate re-typing the entire letter or document.

There is a hidden risk in the new media, in that they have enabled us to bypass the correction and finalizing phases of letter writing, often resulting in quick and efficient dissemination of poorly planned, sloppy and confusing prose.

In technical communications, where complex and potentially important ideas are exchanged, clearness of expression is obligatory. I could cite, nevertheless, many examples (some from recent RISKS, which I will not include to avoid unfairly embarrassing the authors) where bad writing has rendered sentences unintelligible and thoughts and ideas obscure.

We tend to be very quick to correct each other on points of technical accuracy, but very slow to correct, or even recognize, inaccuracy of expression in our own or others' writing.

While I do not advocate abandoning the ASCII keyboard for quill and parchment, I do encourage readers of RISKS to take the time to proof and revise any of their writing meant to convey important technical information.

Re-read your work, and have others examine it for clarity, absence of jargon, and general comprehensibility before you send or submit it to anyone. Remember that word processors and email facilities are only tools, and that the burden of effective communication still rests upon those who use them.

Bruce A. Sesnovich   mcnc!rti-sel!dg_rtp!sesnovich
Data General Corp.   suntoo!dg_rtp!sesnovich@sun.com
Westboro, MA   "The rest is silence, musically speaking"

[This message gets a HEARTY ENDORSEMENT from the RISKS COORDINATOR. I am horrified at some of the messages that I get. I do reject some solely on the grounds of general incoherence. (I stated initially that I would not tamper with messages, but occasionally I do fix a horrible "mispelling". Being an inveterate punster, I am attuned to ambiguities; however, I notice that most people do not notice them (the ambiguities, not the people).

Bruce's message is relevant to RISKS. Just as ambiguities in program specifications can cause serious risks, so can ambiguities in discussions. Much of the lay understanding of systems and computers -- particularly for something like Star Wars -- is based on sloppy reasoning, misrepresentation, misunderstanding, and so on. If we can't take some care in writing what we think we meant to say, then it may not be worth writing -- or reading. PGN]

Words, words, words...

Mike McLaughlin <mikemcl@nrl-csr>
Sat, 3 May 86 13:06:29 edt

Many words have appeared here and in the press on topics such as SDI, Chernobyl, and other matters. At least in this forum, we should be careful of what we say, and what we think others mean when they say something. To quote my favorite source, The American Heritage Dictionary of the English

Language:

deceit - Misrepresentation; deception. A strategem; trick; wile.

deceitful - Given to cheating or deceiving. Misleading, deceptive.

deceive - To delude; mislead. _Archaic:_ To catch by guile; ensnare.

Synonyms: deceive, betray, mislead, beguile, delude, dupe, hoodwink, bamaboozle, outwit, double-cross. These verbs mean to victimize persons, for the most part by underhand means.

error - An act, assertion, or belief that unintentionally deviates from what is correct, right, or true. The condition of having incorrect or false knowledge. A mistake. The difference between a computed or measured value and a correct value.

Synonyms: error, mistake, oversight. These nouns refer to what is not in accordance with truth, accuracy, right, or propriety. Error is clearly preferable to indicate belief in untruth or departure from what is morally or ethically right or proper. Mistake often implies misunderstanding, misinterpretation, and resultant poor judgement... Oversight refers to an omission or a faulty act that results from... lack of attention.

lie - A false statement or piece of information deliberately presented as being true; a falsehood. Anything meant to deceive or give a wrong impression. To present false information with the intent of deceiving. To convey a false impression. To put in a specific condition through deceit.

mislead - To lead or guide in the wrong direction. To lead into error or wrongdoing in action or thought; influence badly; deceive.

See synonyms at deceive. Misleading, deceptive, delusive. Misleading is the most nonspecific... it makes no clear implication regarding intent. Deceptive applies... to surface appearance, and may imply deliberate misrepresentation. Delusive stresses calculated misrepresentation or sham.

mistake - An error or fault. A misconception or misunderstanding. To understand wrongly; misinterpret. To recognize or identify incorrectly. Wrong or incorrect in opinion, understanding, or perception. Based on error; wrong...

See synonyms at _error_.

I have condensed the definitions and discussions somewhat. The point is that a person who believes something, however erroneously, and espouses and publicly supports that belief, is *not* lying. These are complex times. There are many matters about which reasonable persons, even reasonable scientists, may differ. There is no point in saying that a person lied when that person was doing the best work possible based on the knowledge and belief available at the time. It significantly interferes with rational discussion - it not only interferes with cooperative searches for the truth, it nearly eliminates any chance that the truth, when found, will be accepted.

Copyright Laws

<Matthew_Kruk%UBC.MAILNET@MIT-MULTICS.ARPA>
Fri, 2 May 86 09:24:24 PDT

From the Thursday May 1st issue of the Vancouver Sun (Vancouver, British Columbia):

Copyright laws apply to software: court

Waterloo,Ont. - Canada's 50-year-old copyright laws, created to protect artistic works such as music and literature, also cover computer programs, the Federal Court of Canada has ruled in a decision believed to set an international precedent.

Although the verdict can be appealed, it is thought to be the first case anywhere in which legal dispute over rights to software has gone to trial. Similar cases in Britain, Australia and the U.S. have concluded with pre-trial injunctions against software pirates.

In a decision this week, Justice Barbara Reed ruled in favour of Apple Computer Inc.

Apple lawyer Alfred Schorr said the company cited the copyright law in suing "a very large number of defendants" involved in assembling and selling computers that were virtually identical to the Apple II.

A central issue was whether programs encoded electronically on silicon chips are simply pieces of hardware or in fact represent intellectual property that should be viewed as "literary works", Schorr said.

The defendants are prohibited from assembling and offering for sale computers or component parts that infringe on the two basic operating programs used in the Apple II.

Re: Correction on Challenger

<mooremj@eglin-vax>
0 0 00:00:00 CDT

> [From Jeff Siegal]
> It is stated in the original column that Dr. Doering's observation
> _was_ made when he watched the videotape, not months later, as Mr.
> Moore claims.

I did not see the original article and the time element was not clear from the excerpt. Thank you for clarifying this. I withdraw the comment in question.

/mjm

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 2: Issue 49

Tuesday, 6 May 1986

Contents

Perrow on reactor containment vessels

Richard Guy <guy@LOCUS.UCLA.EDU>
Wed, 7 May 86 17:27:54 PDT

I found the following paragraph to be particularly prophetic: (p.40-1)

"We can be glad that we have containment buildings. These are concrete shells that cover the reactor vessel and other key pieces of equipment, and are maintained at negative pressures--that is, at a lower air pressure than the atmosphere outside of them--so that if a leak occurs, clean air will flow in rather than radioactive air flowing out. The Soviet Union, which did not begin a large nuclear generating program until about 1970, is far less concerned about the chance of large accidents, so they did not build containment structures for their early reactors, nor do they yet require emergency core cooling systems. Had the accident at Three Mile Island taken place in one of the plants near Moscow, it would have exposed the operators to potentially lethal doses, and irradiated a large population."

How is negative pressure maintained? By pumping the contents of the containment building outside? Into a tank somewhere? It seems to me that a leak in the reactor vessel would be releasing very hot gases at very high pressure into the containment building, and even though the building is much larger than the vessel, the pressure differential could be eliminated very soon. To answer my initial question, it seems that the only safe place to pump the (possibly contaminated) building contents is into tanks inside the containment building. Does anyone know if this is how its done?

Richard Guy   Excerpt from: Normal Accidents, by Perrow
UCLA Computer Science   1984, Basic Books

[The Soviets are putting the blame on human error. But that may be the case only because they are not very computerized. However, as in TMI, one can put some blame on the absence of computers! In nuclear power, you seem to run the risk of losing either way!]

Captain Midnight

Scott Dorsey <gatech!gitpyr!kludge@seismo.CSS.GOV>
Sat, 3 May 86 18:30:55 edt

Assuming that Captain Midnight was not an employee of HBO, the trouble required to override a satellite signal is still pretty complex. A significant amount of power is required, probably from some travelling wave tube or klystron. High-power microwave stuff is often sold government surplus at pretty low prices, and a kilowatt or so would certainly do the job. Modulation of equipment designed for pulse and similar radar applications would not be simple, though, and from the look of the bad signal that the Captain put out, that may well have been the method used. Large dish antennae are pretty common, and mesh antennae can be put up and taken down in an hours time, and constructed of wood and chicken wire.

In addition, it is possible that the signal originated from somewhere inside HBO. Several examples exist of the wire feed from a radio station's studio to their transmitter being cut and replaced with casette players, etc. In addition, if the studio/transmitter feed is a 2.6 GHz micro link, it is pretty trivial to intercept and jam.... It is possible that off-the-shelf Gunnplexers, and similar low-cost low-power transmission equipment could be used.

Of course, there is always the possibility that a disgruntled HBO employee had a little bit of fun...

>From the Land of Ted Turner

Scott Dorsey " If value corrupts
kaptain_kludge then absolute value corrupts absolutely"

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

---

Capt. Midnight & HBO

<sdcsvax!sdcrdcf!burdvax!psuvax1!psuvm.bitnet!mrb@psuecl.BITNET@ucbvax.berkeley.edu>
3 May 86 03:54:44 GMT

Well, it takes a little more than just a home TVRO outfit to break in on HBO. Capt. Midnight had two possible places of entry: 1.) on the microwave path(s) between HBOs origination point and their uplink transmitter (which I think is on Long Island, but not sure)......or, 2.) by double illuminating their satellite transponder which is actually carrying the program. Double illuminating is a fancy way of saying "broadcasting over top of them".

During a double illumination, when both signals are about the same power level as received by the satellite, they just mix together. I suppose if one was much more powerful than the other, it would "capture" the channel; it is F.M., after all. However, what most likely happened is that the HBO uplink staff was monitoring their return signal from the satellite. For C-band satellites like Galaxy, Westar, Satcom, etc., you send the signal up at 6 GHz. and the satellite rebroadcasts it back down at 4 GHz. Uplinks routinely send & receive simultaneously in order to monitor their signals. In any event, they probably saw that somebody was uplinking on their transponder.....this is not a totally unknown phenomenon; in fact, it happened on a PBS show not too long ago (Sherlock Holmes, I think). There are lots of video uplinks out there...some operated by Western Union, RCA, etc....others by PBS stations in Hartford, Denver, Miami, Columbia S.C., etc. or the PBS Master Origination Terminal near Washington, D.C.......still others by the bigger commercial stations for newsgathering, etc. (Metromedia, INN, etc.). Every once in a while, somebody in operations slips up and starts transmitting on an occupied channel. Well, standard procedure says that you turn off your uplink signal to the satellite, which leaves just the "bad guy". Then it should be easy to identify who(m) it is.

This is most likely what happened when viewers saw a scrambled mess, and then just the Capn's message. Of course, he didn't stay on much longer after that. However, every uplink is a known quantity licensed by the FCC...I don't know of any backyard ones (yet) due to the fairly high-power amplifier and specialized microwave gear required. So we can limit the possible suspects down to the people who were working that night, or had access to the sites. The type of character generator (electronic typewriter) used to produce the message graphics limits it further...only a few uplinks probably have this kind of character generator. Also, many uplinks put an identification code in the vertical interval (the black bar that rolls through the picture when the vertical hold is messed up)...for example, PBS uses a binary number pulse to identify their uplinks. If the guy wasn't smart enough to disable or delete the VITs, well...methinks they got him (not likely though). Also, all color bars are not alike when carefully examined, in terms of bar widths, etc. and I'm sure those few seconds of signal are being pretty thoroughly torn apart.

This of course presupposes that he did it on the uplink to the satellite, not on the microwave path. A good question that remains is: Was his signal correctly scrambled so that all the descramblers would let it through (HBOs video scrambling is not particularly sophisticated, unlike their digital audio encoding...he didn't transmit any audio program)? Or do descramblers let "normal" signals through O.K. .... I don't think so.

Let's see some discussion on this! (Sorry the above was so lengthy.) Personally speaking, it was a neat stunt but he better have covered his tracks pretty well.

MRB@PSUECL

NSA planning new data encryption scheme - they'll keep the keys

Jon Jacky <jon@uw-june.arpa>
Sun, 4 May 86 22:20:58 PDT

The following excerpts are from a New York Times story "Computer code shift expected - eavesdropping fear indicated," by David E. Sanger, April 15, 1986, pps 29 and 32. The story described plans by the National Security Agency (NSA) to replace the current Data Encryption Standard (DES) with a new system of its own design. The story said that the system would be phased in beginning January, 1988. Speaking of DES, the story said,

"While the government helped design (DES), it has no special advantage in determining a particular key being used. ... Security experts say there have been no known successful efforts to defeat (DES). ... But NSA officials have said that they do not want to entrust a rising volume of sensitive data to a coding system whose major elements have been widely published for some time.

Details of the new system are still unclear. But ... unlike the Data Encryption Standard, the new algorithms will not be publicly available. Instead, they will be buried in computer chips manufactured to NSA specifications, and encapsulated so that any effort to read the code with sophisticated equipment would destroy the chip.

... By some accounts, under the new system the NSA would distribute the keys -- probably limiting them to companies in the United States. ..."

The story explained that NSA wanted the system to be adopted by industry as well as the Federal government, and if institutions like the Federal Reserve system adopted it, banks and other private institutions would be encouraged to follow suit.

I know little about data security and encryption, but these points seem interesting:

1. NSA appears concerned that DES may become compromised in the near future.

2. NSA apparently believes that greater security can be assured by keeping the encryption algorithm secret. Could this not lead to a false sense of security by preventing independent researchers from pointing out weaknesses that NSA is unaware of or unwilling to divulge? Is it reasonable to assert that hardware can be built so that no test equipment can probe it?

3. What about keeping the keys under NSA control? At the very least, it could create logistical difficulties; at worst, it seems to permit NSA to snoop at will.

-Jonathan Jacky University of Washington

Espionage

Mike McLaughlin <mikemcl@nrl-csr>
Mon, 5 May 86 08:45:37 edt

U.S. Naval Institute Proceedings, May, 1986 (Naval Review issue) has an excellent article by Bamford on the Walker case. Also has a summary of Navy espionage cases since 1981.

- About 20 Navy/Marines charged in last five years.
- Not one was "recruited" - all approached the bad guys.
- All did it for money.
- Although no case involved "computers" a number were "computer-like", i.e. crypto & telecommunications.

Heartily recommend all compusec types read, and think.
- Mike McLaughlin

The Star Wars Swindle

Peter G. Neumann <Neumann@SRI-CSL.ARPA>
Sun 4 May 86 21:10:34-PDT

Dave Weiss passed along the following quote from Harper's, May 86, from an article by Fred Reed entitled "The Star Wars Swindle":

> "The comprehensive vagueness of Star Wars is, insanely, allowing a technical question - Will it work? - to be answered by an ideological show of hands."

Backups

Will Martin <wmartin@BRL.ARPA>
Wed, 7 May 86 11:14:34 EDT

The issue of backup procedures, difficulties, and methodologies has been
discussed amongst those of us at this Activity and at other parts of the
Army Materiel Command for some time now, mainly in the context of our
acquiring and proliferating small workplace-automation computers which are
located in the users' offices (as opposed to being in traditional computer
centers), and where the systems administration tasks (which would include
backup) are performed by functional specialists who are (usually) not
computer experts or in computer-related job classifications. Though we have
discussed it, there really has been no good and elegant solution to the
problem(s). Most of these machines are backed up on cartridge tapes, with a
daily incremental and weekly full user-filesystem schedule (and monthly for
the entire system). When you then get into the issue of PC's, where you do
not have an assigned system administrator, the whole thing really breaks
down. If you have the luxury of having all your PC's on some network and can
run some sort of background task at odd hours, which backs up data to some
other storage system from each PC, that is great. (We don't have this, and I
don't know of anyone who does.)

One other thing I think we need more of, considering how the existence of
fresh backups cannot be relied upon, is more and better tools to get around
failures. Tools that will let a user get to the data on his hard disk even
after it has nominally been "deleted", or special hardware that will let
someone read data off a disk that has been damaged or trashed by some glitch
or another -- we all know that the bits are still there on the medium; it is
just the paths to get to them that are damaged and garbaged by failures. I
believe that there are firms who do this on a contract basis now; we
probably need to implement this expertise in devices and programs that are
usable by less-skilled people. Of course, the existence of such tools will
create security holes, also -- something that can dig down into the guts of
a disk this way would also bypass copy-protection or use-restriction, and
make the illicit recovery of data thought to be erased possible. I think we
will have to accept such risks to gain the capability to recover
irreplaceable data or work.

Will Martin
USArmy Materiel Command Automated Logistics Mgmt Systems Activity

UUCP/USENET: seismo!brl-smoke!wmartin or ARPA/MILNET: wmartin@almsa-1.ARPA

Interpreting Satellite Pictures

"Lindsay F. Marshall" <lindsay%cheviot.newcastle.ac.uk@Cs.Ucl.AC.UK>
Wed, 7 May 86 10:12:02 gmt

Sir - "We have never had to interpret this kind of satellite picture
before...... we may have got it wrong" (U.S. Government scientist, in the
Guardian Letters, Sat. 3rd May 1986)

(Could this be relevant to SDI?)

Word-processing damages expression

Niall Mansfield <MANSFIELD%DHDEMBL5.BITNET@WISCVM.WISC.EDU>
Tue, 06 May 86 13:14:59

In RISKS-2.48, Bruce A. Sesnovich asked whether word processing and electronic mail are helping to proliferate bad writing. Surely, YES! The following is a list of the more interesting spellings noticed on the net, excluding what I thought were obviously typos.

[I have used the words on Bruce's list to write a nonsense paragraph:

I beleive Britian is definately not compatable reguarding cleen explainations. I was woundering if it is truely nessesary to let lose a concious warrantee which is to periferal too guarentee a miscellaney of usefull ideas. The kernal idea is a distructive facination for publically loosing ones bargins. (No Deniall)?

By the way, I added the hyphen in the SUBJECT: line, to remove one of its several ambiguities... PGN]

Re: Word-processing damages expression

Peter G. Neumann <Neumann@SRI-CSL.ARPA>
Wed 7 May 86 10:33:54-PDT

One way of judging RISKS contributions is by how sloppy the spelling is. One might assume that a miserable speller would be a sloppy thinker. However, there is grave danger therein -- as some of our most intuitive and forward-thinking (right-brained) folks are miserable spellers. As someone who has always been a good speller, a good grammarian, and so on, I resist an instinctive suspicion of miserable spellers, mantaining the patience to dig beneath the surface to seek worthwhile ideas lurking. But please try harder to make my task easier -- by writing more coherently and spelling halfway decently.

Peter

Proofreading vs. computer-based spelling checks

Dave Platt <Dave-Platt%LADC@HI-MULTICS.ARPA>
Tue, 06 May 86 13:10 PST

There has been some discussion in the SF-Lovers digest of late about this basic subject... people have been submitting mention of their "favorite typos". Several people have noted that some recent books have been coming out with some glaring errors: words that are correctly spelled, but are entirely wrong for the context in which they appear. Frequently, these words are either (a) similar in sound to the word that "should have" been there, or (b) can be generated from the correct word via a simple permutation of letters, addition or deletion of a letter, etc.

It appears that some publishers are accepting manuscripts in machine-readable form (disk or download), running them through a spelling checker, and then printing them without actually having them proofread by a reasonably literate reviewer. I don't know the details... perhaps they have completely eliminated the author's galley copies, or perhaps some authors just aren't taking the time to proofread the galleys (or having someone other than themselves do the proofread to catch errors of this sort).

I seem to recall a passage in "Imperial Earth", by Arthur C. Clarke, concerning the pitfalls of cybernetic voice-to-type memowriters about 150 years in the future. He wrote that everybody who uses (will use?) such systems was careful to proofread the output of the voice-recognition modules, as some "hilarious" malaprops had occurred during the early years of these systems' availability.

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 2: Issue 50

Thursday, 8 May 1986

Contents

Refocus the discussion, please!

<estell@nwc-143b>
8 May 86 12:44:00 PST

I want to discourage RISKS contributors from discussing at length how Capt. Midnight jammed the HBO signal - UNLESS there is reason to suspect that (mis)use of computers was a contributing factor. Similarly, I want to discourage the continued discussion of the Challenger disaster, unless there is reason to suspect that computer error - or human error of omission because of reliance on computers - contributed materially to the failure.

Up to a point, these discussions are relevant; they demonstrate that we can not trust our lives naively to fully automated systems. SDI, BART, FAA, NYSE, etc. must be aware of that. As computer professionals, we have the duty of admitting our own humanity, and the frailty of our creations. Otherwise, the sophisticated technology can fool the public too easily.

Instead, I would encourage RISKS contributors to pursue topics like data encryption, which appeared recently [RISKS 2.49]; and to wrestle with the question raised by Dave Weiss in that same issue, viz. CAN Star Wars ever be made to work? Kept in technical focus, this question could lead to research and application of genuine benefit.

It is very easy for us, the readers and contributors, to rely on the moderator to filter our contributions. But I think it unfair to put him in the position of sorting lots of interesting items of questionable relevance. To the extent that these topics (including the ones that interst me) should be pursued, perhaps that should occur in another electronic forum. Comment?

Bob

Refocus the discussion, please? Also, Delta rocket shutdown.

Peter G. Neumann <Neumann@SRI-CSL.ARPA>
Thu 8 May 86 20:02:32-PDT

Bob, Thanks. Contributor self-discipine is greatly appreciated. However, when in doubt about a contribution, I have a bias toward the holistic view -- we are using computers to control physical environments, and relying on ordinary mortals to do it. RISKS exists because of the computers and communications. But we must not forget the global nature of the problems.

Captain Midnight reminds us again of a type of communication vulnerability that is vastly more widespread than many of our readers suspect. The Challenger disaster (28 Jan) is only the tip of an iceberg, although RISKS has not had much on it lately -- or on the Titan 34D (18 Apr) or the Delta rocket (3 May). (We hope that the Atlas-Centaur fares better on 22 May, in which case it might get dubbed the At-Last-Centaur! Fortunately, it is NASA's most reliable, with 43 successful launches dating back to September 1977.)

The type of issue that I raised after the Challenger disaster regarding the possibility of accidental or malicious triggering of self-destruct mechanisms in general recurs in a slightly different form in the Titan 34D failure, in which the rocket's main engine mysteriously shut itself down 71 seconds into the flight -- with no evidence of why! (Left without guidance at 1400 mph, it had to be destroyed.) The flight appeared normal up to that time, including the jettisoning of the first set of solid rockets just after one minute out. Bill Russell, the Delta manager, was quoted thus: "It's a very sharp shutdown, almost as though it were a commanded shutdown." Could this have been an accidentally generated internal shutdown signal (software bug or comm interference)? (There was no evidence of a transmitted shutdown, so it is was very unlikely that it was maliciously generated.) Before you answer, recall the local CB interference problem on automobile microprocessors, the microwave side-effects on pacemakers and other devices, RF interference on computer buses (an older problem), the alleged Sheffield communication interference problem, etc...

Peter

Large systems failures & Computer assisted writing.

Ady Wiernik <wiernik@nyu-acf8.arpa>
Thu, 8 May 86 16:36:07 edt

I hope that I'm not contributing to much to the (growing) link between the risks forum and net.sf-lovers; However, please let me add my two-cent worth of comments:

1. In his article, Dave Benson <benson%wsu.csnet@CSNET-RELAY.ARPA>
   asked:

> From: Dave Benson <benson%wsu.csnet@CSNET-RELAY.ARPA>
> Subject: Normal Accidents and battle software
>
> >According to
> >
> >   Charles Perrow
> >   Normal Accidents: Living with High-Risk Technologies
> >   Basic Books, New York, 1984
> >
> >we should expect to see large-scale accidents such as the loss of the
> >space shuttle Challenger. Perrow's thesis, I take it, is that the
> >complexity of current technology makes accidents a 'normal' aspect
> >of the products of these technologies.
> >
> >We may view space shuttles launches, nuclear reactors, power grids,
> >transportation systems, and much real-time control software as lacking
> >homeostatis, "give", forgiveness. Perhaps some of these technologies
> >will forever remain "brittle".
> >
> >Questions: Does anybody have a good way to characterize this brittleness?
> >To what extent is existing battle software "brittle"?

The question was beautifully answered in a science-fiction book named "Dome" (I don't remember the Author's name). In this book, a large fast-breeding reactor was built in Pittsburgh, and on the day before the ceremonial opening, it had a meltdown-like accident as result of malfunction in the control computers caused by human errors. The story contained many other things, but the interesting point (at least to readers of this forum) is that in the story a young mathematician had predicted before the reactor accident that such an accident would happen, (within a predicted time from the start of operations), based on calculations related to the complexity of the nuclear power-plant and to the laws of probability theory. His opinion was suppressed by the power-company officials (he used to work there).

The "brittleness" is related to the amount of interdependencies between the various subsystems of the power-plant and the chance of failure of each sub subsystems. This argument is similar to the argument made in this forum about the operation of SDI.

2. In another article, Dave Platt <Dave-Platt%LADC@HI-MULTICS.ARPA>
    (why are there so many Dave's on this forum? Is HAL9000
    responsible? :-) states:

> Date: Tue, 06 May 86 13:10 PST
> From: Dave Platt <Dave-Platt%LADC@HI-MULTICS.ARPA>
> To: Risks@SRI-CSL.ARPA
> Subject: Proofreading vs. computer-based spelling checks
>
>   [Edited out - related to typos in current SF literature]
>
> I seem to recall a passage in "Imperial Earth", by Arthur C. Clarke,
> concerning the pitfalls of cybernetic voice-to-type memowriters about 150
> years in the future. He wrote that everybody who uses (will use?) such
> systems was careful to proofread the output of the voice-recognition
> modules, as some "hilarious" malaprops had occurred during the early years
> of these systems' availability.

A similar gadget is used in the second book of Issac Asimov's Foundation trilogy (Foundation and Empire). In this book, the differentiation between words with similar pronunciation was done using the accenting of the word, and even then the machine has to be corrected sometimes.

                        Ady Wiernik.
In two weeks: ady@taurus.BITNET or: ady%taurus.BITNET%wiscvm.ARPA

DESisting

<dm@BBN-VAX.ARPA>
08 May 86 14:07:35 EDT (Thu)

There was an article in Science about this several months ago (perhaps it was just in the proposal stage then, and now is fact, or maybe it was a slow news day at the Times...).

Since the volume of data transmitted using DES is so large, and the information protected by it is so valuable (e.g., HBO audio tracks..., Department of Agriculture Hog reports, electronic funds transfers between Federal Reserve Banks...), NSA now feels that it is worthwhile for someone to spend, e.g., $10 billion to build a DES-breaker, because the potential payoff will be so great. For that reason, they intend to decertify DES by 1990.

To replace DES, NSA will offer their own little encryption boxes, with secret encryption algorithms, and possibly protected so that snooping will destroy the evidence of the encryption algorithm. They will offer several different kinds of encryption boxes, using several different algorithms, so that there won't be so much reliance on a single algorithm.

What about keys? Well, in decreasing order of security (says NSA, disingenuously), you can buy them from NSA, I think you can buy instructions on how to make up your own keys from NSA, or you can make up your own. Buying them from NSA is more secure because NSA knows the pitfalls of the algorithms, knows the general pitfalls of key generation, etc. Of course, if you buy the keys from NSA, maybe NSA keeps a copy of the keys, and maybe they'll use their copy to keep tabs on what you're encrypting...

DESisting (RISKS-2.49)

Wm Brown III <Brown@GODZILLA.SCH.Symbolics.COM>
Thu, 8 May 86 13:35 PDT

> RISKS-LIST: RISKS-FORUM Digest, Tuesday, 6 May 1986 Volume 2 : Issue 49
> From: jon@uw-june.arpa (Jon Jacky)
> Subject: NSA planning new data encryption scheme - they'll keep the keys

My own knowledge of cryptology is limited and mostly theoretical, however there are some additional bits of information available in public domain literature which lead me to draw slightly different conclusions from this news item.

> The following excerpts are from a New York Times story "Computer code shift expected - eavesdropping fear indicated," by David E. Sanger, April 15, 1986, pps 29 and 32. The story described plans by the National Security Agency (NSA) to replace the current Data Encryption Standard (DES) with a new system of its own design.
>
> Details of the new system are still unclear. But ... unlike the Data Encryption Standard, the new algorithms will not be publicly available. Instead, they will be buried in computer chips manufactured to NSA specifications, and encapsulated so that any effort to read the code with sophisticated equipment would destroy the chip.

It is a long-standing ground rule of the crypto biz that the adversary will sooner or later obtain the basic algorithm used in any cypher system. Traditionally, security is **always** based only on the knowledge of keys, not on keeping the theory of operation secret.

A system which depends upon the secrecy of its algorithm is effectively a single-key code. Eventually it will be compromised and the other side will be able to read all those tapes of encrypted messages which they have been saving. Unless everything ever sent over the system has gone stale by that time, this is generally an unacceptably large loss. Not the way to design a system for long-term use.

By the time such a system is in general use, there will be many thousands of devices in circulation and hundreds of people who know how it works. Sooner or later, the guys in black hats will get hold of one or the other and pry the top off to find out what's inside. It may be possible to make the packages tamper-resistant, but tamper-PROOF is a big order (ask the makers of Tylenol).

> ... By some accounts, under the new system the NSA would distribute the keys -- probably limiting them to companies in the United States. ..."

Many recent systems use keys consisting of very large numbers chosen from a set which is too large to try exhaustively (100 digit primes, cubes, etc.). This category includes most of the "Public Key" cryptosystems (in which the encryption and decryption keys are different.) It seems very possible that

NSA intends to create a subset (still very large) of some such class and then distribute devices with these individual keys built into them. Disassembling such a chip would compromise only one possible key from a large universe, and few if any humans can remember many such keys, eliminating that source of risk.

One of the fringe benefits (from NSA's viewpoint) is that they would know the entire universe of assigned keys. An outsider would have to try all of the theoretical possibilities, however NSA could exhaustively try every one of a few millions relatively quickly.

Re: Failure to Backup Data

Greg Brewster <brewster@nacho.wisc.edu>
Thu, 8 May 86 11:25:28 CDT

I must agree that the importance of regular backup of data on microcomputers is very much underemphasized to many nontechnical users. However, in cases where individuals are solely responsible for particular data files (as in the example of a scholar using a microcomputer to write a book), I don't believe that incremental backups are prohibitively difficult.

As Jim Coombs correctly states in RISKS-2.48
> Since a complete backup of a 10
> megabyte hard disk on an IBM XT can take a half-hour, I am sure that backing
> up a 40 megabyte hard disk on a workstation will require more time (and
> diskettes) than the majority of our scholars will invest.

However, there is absolutely no need for any single scholar to be concerned with a complete epoch dump of a 40 megabyte hard disk. The data files for most books will fit on one or two floppy disks. I believe that, if the dangers of data loss were emphasized enough, any writer would be happy to copy each day ONLY the files s/he changed on that day. If the microcomputer has a reliable clock and files are marked with modification times, then any experienced programmer could write a simple command file to back up all the files changed during the time the current user has been logged in automatically.

This is a case where the risk of data loss can be decomposed into a risk of loss of particular data for each system user. I believe a reasonable approach then is to require each user to deal with his/her 'individual risk' as s/he wishes. However, the magnitude of this risk of data loss must be emphasized to inexperienced users.

Greg Brewster brewster@nacho.wisc.edu (ARPA)
University of Wisconsin - Madison ..ihnp4!uwvax!brewster (UUCP)

Search RISKS using swish-e

Report problems with the web pages to the maintainer

Search RISKS using swish-e

THE RISKS DIGEST

Forum on Risks to the Public in Computers and Related Systems

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

Volume 2: Issue 51

Sunday, 11 May 1986

Contents

Reliability limits

Brian Randell <brian%cheviot.newcastle.ac.uk@Cs.Ucl.AC.UK>
Fri, 9 May 86 10:28:52 gmt

I have for a number of years held, and expounded, the opinion that: "If one automates a complex manual system, which is being carried out reasonably competently, then the very best that one can hope to achieve is fewer but BIGGER errors".

To give a couple of low-key illustrations: an automated payroll system can normally be expected to get virtually all of its calculations exactly correct - but have you ever heard of a manual payroll system producing a paycheck for $999,999.99 or for $0.00? When a newspaper goes over to computerized type-setting one normally sees a considerable drop in the number of typos, but the sudden appearance of occasional major errors - e.g. instructions to the formatter in capitals in the middle of a paragraph, whole sections in completely the wrong font, etc.

The thinking behind my statement is that, compared to computer-based systems, humans usually have a great ability to recognise an unusual situation, and to use their general knowledge of the world in assessing its correctness, and its possible consequences.

I now no longer have any idea whether the statement is one that I have plagiarized from someone else, and often find that people find it illuminating as well as believable, and that it is a good way of injecting a note of caution into the more naive and over-optimistic discussions that often take place concerning possible new computer-based systems.

I would be most interested to see how the RISKS forum reacts to it - always assuming that something along this lines has not already been the subject of a debate which took place before I became a subscriber.

Brian Randell - Computing Laboratory, University of Newcastle upon Tyne

ARPA : brian%cheviot.newcastle@ucl-cs.arpa
UUCP : <UK>!ukc!cheviot!brian

NSA assigning encryption keys

<ELINSKY@IBM.COM>
9 May 86 10:55:02 EDT

In light of all the recent spy cases, if the NSA keeps records of the keys it has assigned to users, there's the risk that someone with access to them might sell them "for the right price". The keys would be worth so much that a would-be intruder could offer an irresistibly high price to the right individual, and still come out ahead.

Jay Elinsky, IBM T.J. Watson Research

HBO pirate

Lauren Weinstein <vortex!lauren@rand-unix.ARPA>
Thu, 8-May-86 11:00:05 PDT

Let me preface this by mentioning that my consulting includes work with the company that uplinks WTBS to the bird, and that I have some experience in the details of satellite uplink technology.

Just briefly:

The odds are very high that the HBO pirate was at a commercial uplink facility. A variety of technical considerations (which I won't go into here) make it very unlikely that a terrestrial microwave path was involved. The signal quality put out by the pirate was actually quite good. He had to run 10db more power than the HBO uplink to capture, which is a fair amount of juice. This was probably made possible by the fact that most uplink operators have tended to run much less power than they have at hand on site since new transponders are very sensitive. I think you can bet HBO is running full power on their uplinks now! The character gen used by the pirate was clearly of a standard commercial type that would be located at virtually any site with uplink facilities. Also, it should be noted that when the pirate's "in the clear" signal captured the scrambled HBO uplink signal, the far-end decoders noted the loss of scrambling and switched back into "normal" video passthru mode with scrambling off. It would be trivial for the pirate to disable any ID on the colorbars by throwing one switch. In fact, many uplinks never use such IDs at all.

Actions being taken to catch the pirate have supposedly included checking the logs of many licensed uplink facilities to find out who was on duty at the suspect time. In fact, there are already rumors that the pirate has been caught and fired by his company, but this has not been confirmed. If he (or she) is still unknown, however, the most likely way they'll be caught is if someone starts bragging.

--Lauren--

Re: Failure to Backup Data, by James H. Coombs

Roy Smith <allegra!phri!roy@seismo.CSS.GOV>
Thu, 8 May 86 17:26:01 edt

One thing not mentioned in James's article is what happens when you get a new system which has different backup media than the last one? In our case, that meant switching from 800 to 1600 bpi tape a couple of years ago. We no longer have a drive that can read our old 800 bpi tapes, so we've got all these wonderful archive tapes that we can't do much with.

Of course, there are media-copy services. They may not be cheap, but for the occasional needed file from antiquity, just about anybody can do a raw tape to tape copy for you. But what do you do when your backup media is a 5-1/4" floppy in wombat-DOS verson 6.4 format? Where are you going to get that transfered onto something you can read?

Admissibility of legal evidence from computers

Mike McLaughlin <mikemcl@nrl-csr>
Sat, 10 May 86 13:24:17 edt

In one of my previous incarnations the taxpayers paid me to think small. Specifically, to implement microform (microfilm, microfiche, COM) where-ever it was cost effective. Among other things, we converted about two million personnel records from paper to microfiche. Did lots of good things besides saving money. But, there were certain practical problems...

Personnel records are frequently placed into evidence at court proceedings. With 2,000,000 or so records, each representing a real live (or formerly live) person, several dozen records were in court at any given time. Not to speak of class action suits.

We had researched laws, federal regs, etc.; gotten legal opinions, whatever. There was no question in *anyone's* mind that the records were legal, that the microfiche WAS the record, and that it WAS admissable in any federal court, and in most other courts.

Trouble was, it wasn't readable. Plaintiffs and lawyers do not come equipped with 24X eyesight. Judges and jurors don't either. Ever try to annotate a microfiche? Underline a telling phrase - highlight a key date?

We had to set up a fairly expensive system JUST TO HANDLE COURT CASES. We had to go back to paper (copies for all concerned) in every court case. Worse yet, we had to prove the heredity, ancestry, and legitimacy of the paper copies.

Now, a word to those keeping records on magnetic media, or optical disk, or holographic crystals... Better have a printer handy!

Electronic document media

Mike McLaughlin <mikemcl@nrl-csr>
Sat, 10 May 86 14:09:56 edt

Risks 2.48 contains several items related to electronic document creation and transmission. James Coombs worries about loss of data and loss of tenure due to authors being unaware of some of the discipline necessary for preserving electronic drafts. Bruce Sesnovich and "PGN" are concerned with the poor quality of submissions to Risks, while I mutter about distinctions between mistakes and lies.

I agree entirely with Coombs, but take some exception to Sesnovich and PGN.

1. Editors and proofreaders are not the same - or should not be. The editor reads an author's draft, and assists the author to clarify it, or to achieve some desired end (i.e., making it fit the available space). The proofreader checks the edited draft, ensures that it matches some appropriate style guide, and ensures that the "galley" faithfully reflects whatever the author and the editor have agreed upon. Actually, the old cycle used to be Author -> Editor -> Printer/Typist -> Proofreader -> Pressman/Copier. There were a lot of checks, and a lot of delays. The end product was quality work... as long as timeliness did not matter.

2. Micros, word-processors, e-mail, bulletin boards and electronic forums have abridged the process. Unless PGN or Captain Midnight interpose themselves in the process, the readers of Risks will see exactly what I say, regardless of what I mean. Right out of my head and into the keyboard. The reader gets my half of an extemporaneous conversation. That is both the charm and the risk of e-mail and e-forums.

3. I still have the choice of composing off-line, getting peer review, cor-

recting my work, up-loading it, then proofing the up-load (best done by someone else), and finally transmitting it to PGN. I choose not to do so (but might choose _to_ do so on some other topic or some other day).

In short, I assess the competing demands of spontaneity and perfection, and then act accordingly. My desktop micro, e-mail, and PGN have given me that option. When I started writing, there was no choice.

Bruce, if the computer has done anything harmful to communication, that harm lies in the penchant for excessive iteration of repetitious revisions that squeeze all the juice out of some *person's* thought or opinion until it has no more intellectual appeal than a spare-parts listing.

- Mike McLaughlin <mikemcl@nrl-csr>

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 2: Issue 52

Wednesday, 14 May 1986

Contents

Launch failures

Phil R. Karn <karn@petrus.bellcore.com>
Mon, 12 May 86 03:46:15 edt

There are a couple of minor errors in your mod.risks article. Delta, not Atlas-Centaur, had the streak of 43 successful launches since 1977, and it was Delta-178, not the Titan 34D, whose main engine shut down 71 seconds into flight.

[Blame AP for that one, not me. Never trust what you read in the papers (or anywhere else, apparently)! THANKS. PGN]

I would heavily discount the possibility of a range safety signal causing the failure of Delta-178. There are only two commands available to the range safety officer, ARM and FIRE. The latter causes an engine shutdown alright, but immediately follows it by the detonation of the destruct explosives. The fact that the range safety system worked perfectly 20 seconds after the shutdown indicates that an unauthorized signal is unlikely to have been the cause of the shutdown. Besides, the media has been reporting that the investigation has revealed strong evidence from telemetry of a short circuit in the engine control circuit.

Phil

[Ah, yes, but (a) a short circuit could easily trigger the
shutdown command, and (b) strong evidence could also be wrong.

Well, just for the record, I might as well mention here the misfire
on 25 April (not reported until 9 May) of the Nike Orion, which had
flown successfully 120 consecutive times -- and that was its first
failure. The burned-out Nike first stage failed to separate
before the second stage Orion ignited. Murphy strikes again,
but in spades over recent months. PGN]

brittleness of large systems

Dave Benson <benson%wsu.csnet@CSNET-RELAY.ARPA>

Profoundly, utterly and completely disagree that probability theory can be used to characterize the brittleness of large systems. Using probability theory and mathematical statistics to assess the likelyhood of failure requires experience, enough experience to know the frequency of failure of parts, the frequency of failure of the interaction of parts, etc.

The one big attempt to do this was the Rasmussen report, WASH-(I don't remember the number think it was 1400), which attempted to use fault-tree analysis to predict the failure frequency of large nuclear reactors such as the Three Mile Island set. The actual accident which occured at TMI was not even considered in the Rasmussen report, thus assigned probabilty zero. By twisting the "causes" of the accident at TMI, one might find a probability attached to this accident in the Rasmusen report. Those attempting this have come up with the TMI accident as have an "incredible" probability, i.e., about one chance per billion reactor years.

Nancy Leveson at UC-Irvine is preparing a long survey [mentioned earlier in RISKS] of work on safety related issues in software. She was so kind as to send me a pre-publication version of the report. I highly recommend the finished report to the RISKS readership. It is good. But as Prof. Leveson's survey makes clear, there are no new, good ideas for characterizing brittleness.

She does survey the use of fault-tree analysis for producing reliable software. This technique will certainly help improve the current state of the art in real-time software design. But the Rasmussen report--TMI accident demonstrates that the real world is not (and, I believe, cannot) be completely characterized by such techniques.

Let me remind you that according to Fox, "Software and its Development" the Enroute Air Traffic Control System (a large but not very large real-time C**3-tye system) has to date, only executed about .001 to .003 of all possible paths throught the code.

So, we have not the data to use probability and statistics. Therefore, the brittleness of large real-time software (C**3*I military systems, SDI, major transaction processing software, etc.) needs something else. Here is a thought about that "something else":

The traditional means of studying the most important aspect of our world, people and their societies, has been the humanities. Language, culture, history, writings, anthropology, classics, literature... and do not forget theology, perhaps the subtlest of all. Recently (that is in the last hundred years) these have been supplemented by psychology and the social sciences. This has become possible only AFTER a very long tradition in the humanities.

My suggestion is to study software, large software, with the intellectual tools of the humanists. I would very much like to hear and read what theologians have to say about software. Comments?

[By the way, the AP story of 12 May on Washington State's Hanford nuclear reservation says that in the mid- to late 1940s, thousands of residents may have received doses of radioactive iodine-131 at levels hundreds of times greater than levels considered safe today. Reactors and plutonioum factories "spewed the gas out at levels that today would qualify as a major nuclear accident, thousands of times greater than levels recorded at TMI." The standards have since been changed, but at the time it was apparently considered routine. PGN]

HBO (RISKS-2.49)

Scott Dorsey <kludge%gitpyr%gatech.csnet@CSNET-RELAY.ARPA>
Sat, 10 May 86 11:36:55 edt

I am told by a friend that the HBO studio-transmitter link is a landline. Alhough this cannot be easily overridden with a mobile transmitter, cases exist (like that at the Virginia Tech campus radio station) where the landline was cut along its path and replaced with an originating source (in this case, perhaps a VTR, in the Va Tech case, a casette player).

HBO (RISKS-2.49)

<ihnp4!utzoo!lsuc!dave@ucbvax.berkeley.edu>
Mon, 12 May 86 17:20:53 PDT

To: utzoo!ihnp4!ucbvax!SRI-CSL.ARPA!RISKS
Subject: Re: RISKS-2.49

>   Or do descramblers
>let "normal" signals through O.K. .... I don't think so.

Someone else mentioned on RISKS that they do. I would think they'd have to. Our cable company periodically runs "free Pay-TV weekends" in the hope that viewers will like what they see on Pay-TV and sign up after the free period is over. And paying customers certainly don't have to disconnect their descramblers at such times.

Dave Sherman, Toronto
{ ihnp4!utzoo pesnta utcs hcr decvax!utcsri } !lsuc!dave

Word processing -- reroute [reroot?] the discussion

Chuq Von Rospach <chuq%plaid@SUN.COM>
Mon, 12 May 86 22:44:04 PDT

Word processing and bad english are well within the domain of the group
mod.mag -- you may want to toss a pointer there, and if there is
interest I might put a mailing list on my machine to tie it all up
for the Arpaland.

As someone who publishes a magazine electronically, gets most of its
submissions electronically, and is generally an electronic network
junkie (gotta get my compuserve fix...), they are right. It isn't the
medium in itself, though, but its tendency to let you toss things off
without thinking first (such as this message).

chuq [I should also put in a pointer to COMPUTERS&SOCIETY as a
source of discussion on such topics, for example, a piece
by "Bruce_A._Hamilton.OsbuSouth"@Xerox.COM entitled
ARE ONLINE SYSTEMS HELPING TO PROLIFERATE BAD CODING? Note:
I continue to reject a slew of responses on this topic as too
marginally related to RISKS. Thanks anyway. PGN]

Search RISKS using swish-e

Search RISKS using swish-e

THE RISKS DIGEST

Forum on Risks to the Public in Computers and Related Systems

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

Volume 2: Issue 53

Friday, 16 May 1986

Contents

A late report on the Sheffield -- RFI

Martin Minow, DECtalk Engineering ML3-1/U47 223-9922 <minow%pauper.DEC@decwrl.DEC.COM>
16-May-1986 1241

[PGN's SUMMARY LIST OF HORROR STORIES CONTAINS THIS ON THE SHEFFIELD:
"Exocet missile not on expected-missile list, detected as friend" (SEN 8 3)
[see Sheffield sinking, reported in New Scientist 97, p. 353, 2/10/83];
Officially denied by British Minister of Defence Peter Blaker
[New Scientist, vol 97, page 502, 24 Feb 83]. Rather, sinking abetted by
defensive equipment being turned off to reduce communication interference?]

From the Boston Globe, May 16, 1986:

Phone call jammed antimissile defenses

LONDON -- Electronic antimissile defenses on the British frigate Sheffield, sunk in the 1982 Falklands conflict, were jammed during an Argentine attack by a telephone call from the captain to naval headquarters, the Defense Ministry said yesterday. Twenty crewmen were killed when the Sheffield was sunk May 4, 1982, by a French-made Exocet missile fired by an Argentine plane. A Defense Ministry spokesman, confirming a report in [the] London

Daily Mirror, said Commodore James Salt, the Sheffield's captain, was making "an urgent operational call" to naval headquarters near London when the missile hit. "The electronic countermeasures equipment was affected by the transmission. Steps have been taken to avoid a repetition," the spokesman said. Commodore Salt now has a shore job as chief of staff to the fleet commander-in-chief. (AP)

A late report on the Sheffield -- RFI

<Dave-Platt%LADC@HI-MULTICS.ARPA>
Fri, 16 May 86 17:13 PDT

[beginning of message duplicated the above] From Today's LA TIMES: [...]

> The telephone system's transmitter was on the same frequency as the homing radar of the French-built Exocet missile fired at the Sheffield, and the transmission prevented the Sheffield's electronic countermeasures equipment from detecting the missile's radar and taking evasive action.

The article implies that this situation might have been avoided had the Sheffield been equipped with an uplink into the British satellite communication system; the article gives no details but I'd guess that such an uplink would have used a transmitter which was (a) less powerful, (b) more directional, or (c) on a completely different wavelength.

Does anyone have additional information about the equipment in question?
[Dave Platt]

News items [Lobsters; Eavesdropping]

Alan Wexelblat <wex@mcc.arpa>
Thu, 15 May 86 14:11:13 CDT

Here are a couple of items from today's paper that may be of interest to RISKS readers:

(The following item was discussed in RISKS when the story first broke.)

AWARD REVERSED IN WEATHER DEATH CASE

Boston(AP) - A federal appeals court Tuesday overturned a $1.25 million award to the families of three lobstermen who died in a hurricane the National Weather Service had failed to predict because of an unrepaired buoy.

The 1st Circuit Court of Appeals said the weather service is protected from awards like that made by U.S. District Judge Joseph Tauro because weather forecasting is a discretionary function. [...] Tauro found the government liable in the [fishermen's] deaths because of its failure to repair a weather buoy used to forecast conditions.

In the appellate court ruling, Judge Bailey Aldrich wrote, "The government did not create the weather, it merely failed in the (lower) court's opinion to render adequate performance. "This was a discretionary undertaking."

Michael Latti, attorney for the families, said he would ask the U.S. Supreme Court to review the Appeals Court decision.

He said the 1st Circuit Court found the government did not have to exercise "ordinary reasonable care" when it undertakes a discretionary function such as issuing weather forecasts.

HOUSE PANEL OKS LIMITS ON HIGH-TECH EAVESDROPPING
By Mary Thornton, Washington Post Service

After more than two years of study, a House subcommittee Wednesday unanimously approved a bill that would make it illegal to eavesdrop on electronic communications, including cellular telephone conversations, electronic fund transfers, and computer messages and data transmissions.

The bill would also extend to such communications Fourth Amendment protection against unreasonable search and seizure.

A report by the congressional Office of Technology Assessment last October [...]included a survey of federal agencies, including six that said they planned to intercept or monitor electronic mail as part of their investigative work.

The bill would require a court-approved search warrant for law enforcement agencies to obtain a computer message within six months of its generation and a subpoena after that. [...]

Also, under the legislation law enforcement agencies would have to meet the strict standards of the federal wiretap statute to eavesdrop on cellular telephone conversations.

The bill contains several provisions to make it easier for federal law enforcement agencies to obtain court-approved wiretaps. It would expand the categories of crimes for which a wiretap may be approved as well as the number of officials in the Justice Department who can approve such a request.

The bill also would make it a misdemeanor to use a satellite dish to intercept subscription television signals, but only if the information is then used commercially.

The bill is currently being called "The Electronic Communications Privacy Act of 1986". No HR number was given in the article.

--Alan Wexelblat
ARPA: WEX@MCC.ARPA
UUCP: {ihnp4, seismo, harvard, gatech, pyramid}!ut-sally!im4u!milano!wex

More Phone Bill Bugs...

Dave Curry <davy@ee.purdue.edu>
Thu, 15 May 86 16:14:31 EST

To add to the ever-increasing list of screwed up phone billing software,
this is from the May 12 issue of Communications Week (selected excerpts):

"GTE Sprint Communications failed to bill customers for millions
of dollars worth of calls made between Feb. 21 and April 26 of
this year, Communications Week has learned."

".... cost Sprint between $10 million and $20 million."

"The errors were made through 10 of Sprint's 58 switches...."

"Regular calls.... went undetected in those 10 switches...."

".... $1 billion in revenues a year, $20 million represents about
2 percent of the company's annual revenue."

"The errors apparently happened because programmers made billing
software changes in some, but not all, of Sprint's switches. The
omissions have since been corrected."

Sometimes one wonders if we'll ever learn... I wonder what happens now
to the poor slob who approved those software changes ("ooops.")...

--Dave Curry, Purdue University [davy@ee.purdue.edu]

backup problems

<davidsen%kbsvax.tcpip@ge-crd.arpa>
14 May 86 11:50 EST

Getting people to do backup can be done by management (or whatever passes
for it in educational institutions). The trick is to convince people at
the gut level that there will be consequences if they don't backup.

One method might be to quietly pick people at random, and if their files
are not backed up, pull hardcopy of the work and revoke the user's rights
to use the computer. A really hardnosed management might just randomly
trash a disk now and then (after warning people that this would be done)
and letting the resulting cries of pain get the job done. There will
ALWAYS be those who are too stupid or stubborn to respond to any
education. You might as well either (a) get rid of them, or (b) if they
are really valuable in other ways, assign someone to back up their work.

At one (unnamed) site, management was encouraged to read their electronic
mail regularly by having top management send meeting notices and requests
for data to the middle management. Just one phone call from an irate top

manager asking why a meeting was missed usually did the trick. The middle management started passing the concept on, and now Email is used instead of paper for most messages.

More on backup procedures (amusing ad)

Roy Smith <allegra!phri!roy@seismo.CSS.GOV>
Thu, 15 May 86 21:10:48 edt

There have been several items in RISKS-DIGEST recently about the dangers of not doing backups. I've already made my contribution, but an interesting ad from 3-M caught my eye. As the ad says, "when it comes to doing computer backup, any excuse will do" [i.e. for not doing it -- RHS]. See the June Sci. Am., page 21 for the rest.

BTW, I have no connection with 3-M. I just liked the ad.

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 2: Issue 54

Sunday, 25 May 1986

Contents

Meteorites

Larry West <west@nprdc.arpa>
21 May 1986 2309-PDT (Wednesday)

An article on page 11 of the Wed 21 May New York Times raises an issue I haven't quite seen raised here before. It's only partly related to automation, but that relation is a threatening one.

The article is titled ``Consequences Weighed of Meteorite Explosion'' and reports on the semi-annual meeting of the American Geophysical Union in Baltimore. The article is by Walter Sullivan and is too well-written to condense satisfactorily, but I'll try:

:::::

Meteoric explosions on the scale of the 1908 event in Siberia (12 Megatons) are expected about once per century, and somewhat smaller (but still in the range of nuclear explosions) events should happen more frequently.

Although the US, USSR and Europe could ``probably'' detect that the explosion was non-nuclear, and thus avoid an inappropriate reaction, this would be less true in, say, the Middle (Near) East or India & Pakistan.

``Also, [specialists] said, the response of highly automated systems, such as the proposed Strategic Defense Initiative, could not be predicted.''

Even without a military response, the after-effects could be devastating: filling the atmosphere with sun-blocking particles and curbing food production. Currently, there is roughly a 70-day supply of food on hand in the world [which surprises me -- LW] but a very large meteor could reduce sunlight for two years.

Further, the most energetic explosions will come from those meteors travelling the fastest (and sometimes coming from outside the solar system), and thus the most difficult to predict.

``The discussion took place at a session on natural hazards ... Presiding was Dr. Joseph V. Smith of the University of Chicago, who has been calling for an Internation Decade for Hazard Reduction that would begin in 1990. That effort would be aimed at reducing loss of life, particularly from catastrophes that are on a very large scale but sufficiently rare to have been largely ignored. The plan was first suggested in 1984 by Dr. Frank Press, now president of the National Academy of Sciences.''

``Dr. Smith .... also urged the initiation of an International Decade on Stockpiling for Survival, including development of new techniques for effective, economical storage of ... foods''

Various methods of dealing with a meteor were mentioned, including nuking it and firmly pushing it aside. The main problem is being prepared and being able to reach the meteor in time.

:::::

Hope this hasn't gone too far afield from the focus of this mailing list...

Larry West   USA+619-452-6771
Institute for Cognitive Science   non-business hrs: 452-2256
UC San Diego (mailcode C-015)
La Jolla, CA 92093 USA
ARPA: <west@nprdc.ARPA> or <west@ucsd.ARPA>
DOMAIN: <west@nprdc.mil> or <west@csl.ucsd.edu>

Meteorites, Davis-Besse, Chernobyl, Technology, and RISKS

Peter G. Neumann <Neumann@SRI-CSL.ARPA>
Sun 25 May 86 11:27:51-PDT

Larry West wonders whether his Meteorite contribution has strayed too far afield for RISKS. I think not. One of the biggest risks of using computers in critical environments is that we tend to trust them blindly -- even if the models on which the systems are based are incomplete. In connection with an article on the 46 US Senators who are seeking to cut back the SDI budget, Senator William Proxmire is quoted in the Washington Post of Friday 23 May 1986:

> "Challenger and Chernobyl have stripped some
> of the mystique away from technology."

Some of the blind trust naively placed in technology may lessen for a while after such incidents as the Challenger (together with the other recent NASA difficulties) and Chernobyl. But it always seems to return fairly rapidly, and the lessons are quickly forgotten -- by those who use, depend upon, operate, administer, and regulate the technology. Anticipating the events that might follow the appearance of such a giant meteorite is vital [to avoid administering last Meteor-Rites?]. (This possibility recalls the old case of BMEWS at Thule "recognizing" the moon as an incoming missile.)

As another example of blind trust, the WashPost of Sat 24 May had an article reassessing the Davis-Besse Nuclear Power Plant emergency shutdown last June. "[E]xperts say, Davis-Besse came as close to a meltdown as any U.S. nuclear plant since the Three Mile Island accident of 1979. Faced with a loss of water to cool the reactor and the improbable breakdown of FOURTEEN separate components, operators performed a rescue mission noted both for skill and human foible: They pushed wrong buttons, leaped down steep stairs, wended their way through a maze of locked chambers and finally saved the day last June 9 by muscling free the valves and plugging fuses into a small, manually operated pump not designed for emergency use." [Emphasis on FOURTEEN is PGN's.] The article goes on to describe prior power-company foot dragging and bureaucratic wrangling, despite the lack of a backup pump having been identified as an intolerable risk long beforehand.

The WashPost of Thursday, 22 May 1986 shed a little more light on what happened at Chernobyl. (In case you could not guess, I was in DC for the week.) Could an experiment have gone awry? Human error and/or system error?

> The Soviet Union was conducting experiments to check systems at Chernobyl's fourth nuclear reactor when a sudden surge of power touched off the explosion last month, a Soviet official said ... Soviet officials have said that the explosion happened when heat output of the reactor suddenly went from 6 or 7 percent to 50 percent of the plant's capacity in 10 seconds. The power had been reduced for a prolonged period in preparation for a routine shutdown... "We planned to hold some experiments, research work, when the reactor was on this level," Sidorenko [deputy chairman of the State Committee for Nuclear Safety] said today [21 May]. "The accident took place at the stage of experimental research work."

Peter G. Neumann

London Stock Exchange Computer System Crash

"Lindsay F. Marshall" <lindsay%cheviot.newcastle.ac.uk@Cs.Ucl.AC.UK>
Fri, 23 May 86 09:40:23 gmt

The other day I saw a headline that said the London Stock Exchange had been disrupted by a system crash. There were no more details. Does anybody know anything more??

Lindsay F. Marshall, Computing Lab., U of Newcastle upon Tyne, Tyne & Wear, UK
ARPA : lindsay%cheviot.newcastle.ac.uk@ucl-cs.arpa
JANET : lindsay@uk.ac.newcastle.cheviot
UUCP : <UK>!ukc!cheviot!lindsay

Backup

"Fred Hapgood" <SIDNEY.G.HAPGOOD%OZ.AI.MIT.EDU@XX.LCS.MIT.EDU>
Sat 17 May 86 08:32:13-EDT

What is needed here is a service that will automatically come into your computer at 4 a.m., or whenever, look around inside your hard disk, make a record of the bytes that have changed since the previous night's checkup, and download those to some off-site storage device. Such a system would have the double advantage of being totally automatic and of storing backups off-site, safe from the effects of user stupidity, which is a much better reason for off-site backups than fire or burglary. People worried about security can have the system encrypt everything before the service is allowed in.

[The Get-Rite Backup Company provides an off-the-shelf program that you might want to try. Unfortunately, they were the lowest bidder, and took a lot of shortcuts -- the most important of which is that nothing is ever actually saved. Of course this never bothers you unless you need to retrieve something. Unfortunately, the program was sabotaged by Get-Rite's competitor, Trojan-Horses-for-Stud (to whom "backup" has an entirely different meaning). They lived up to their name, and managed to install a Trojan Horse that, upon first request by you to retrieve a file, simply deletes ALL of your on-line files and then disappears into the woodwork. I hear that they will also take large bribes if you want to wipe out other users' files on demand. PGN]

Backup

Bruce O'Neel <ZWBEO%VPFVM.BITNET@WISCVM.WISC.EDU>
Sat, 17 May 86 12:51 EDT

Re: Management monitoring of backups.

I have a feeling that in educational institutions where the choice is given between hiring someone to do backups for people and "forcing" people to do the backups themselves, hiring someone (undergrad student) will get the nod.

Just a small thought.

bruce (zwbeo@vpfvm.bitnet)

[A THIRD choice usually wins: Do nothing at all until after you get wiped out. PGN]

Search RISKS using swish-e

Search RISKS using swish-e

THE RISKS DIGEST

Forum on Risks to the Public in Computers and Related Systems

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

Volume 2: Issue 55

Wednesday, 28 May 1986

Contents

SDI; Culling through RISKS headers [Message entirely edited]

Jim Horning <horning@src.DEC.COM>
Tue, 27 May 86 11:51:06 pdt

[[Jim and several others called my attention to an article in the NYTimes of 27 May 86, page 9. I have excerpted from the article, as follows. PGN]

"Feasible Computer Control For Missile Shield Doubted"
by Charles Mohr (Special to the New York Times)

"An expert [Jim Horning] in computer programs who was asked to advise on research into defense against long-range nuclear missiles says he is skeptical that a reliable computer system to control such a defense can ever be devised."

The article quotes from a letter from Jim Horning to Douglas Waller (on the staff of Senator William Proxmire):

> "To date no system of this complexity has performed as expected (or hoped) in its first full-scale operational test; no one has advanced any reason to expect that an S.D.I. would either. A huge system that is intended to be used at most once, and cannot be realistically tested in advance of use, simply cannot be trusted."

The article also quotes a statement signed by 36 of the 61 experts who attended a workshop on computing March 16-19 at Pacific Grove CA:

> "The effective defense from nuclear annihilation of the lives, homes and property of the American people, as embodied by the Strategic Defense Initiative (Star Wars), requires highly reliable computer systems of unprecedented complexity. As experts in reliable computing, we strongly believe that a system meeting these requirements is technologically infeasible."

The article notes Dave Parnas' role in the ongoing discussions, and also

> "Lieut. Gen. James A. Abrahamson, the director of the missile defense organization, has said that computer programming was probably the most difficult technical problem faced by his group. But he stresses an optimistic view that it can be solved and argues that Mr. Parnas has applied "unrealistically high criteria"."
>
> Mr. Horning, who like Mr. Parnas has written computer programs for weapons systems, is supportive of Mr. Parnas, observing that "there has been a movement toward Parnas' position" among those knowledgeable about technology.

The article also quotes from Jim Horning's "trip report" to participate in a meeting of the Strategic Defense Initiative Organization (see RISKS-1.2, 28 August 85). END of PGN excerpting.]

[Wow, it is 9 months to the day since RISKS-1.2, and we've had 99 issues (not counting the "pilot issue", RISKS-1.1, on 1 Aug 85). I hope we are not overwhelming you, but I also hope we can keep up the generally good quality of contributions. PGN]

Blind Faith in Technology, and Caspar Weinberger

<LIN@XX.LCS.MIT.EDU>
Sun, 25 May 1986 17:45 EDT

On the blind faith in technology, it is interesting to note that, when initial reports came in after the bombing of Libya that U.S. bombers had hit the French Embassy, Weinberger said,

> "That's impossible. They weren't ordered to do that."

Risks of doing software quality assurance too diligently

Peter G. Neumann <Neumann@SRI-CSL.ARPA>
Wed 28 May 86 21:02:44-PDT

From the Torrance Daily Breeze, 19 May 1986, page 1, courtesy of Chris Shaw:

> Death threats dog fired whistleblower
> (by James Hart, Aerospace writer)
>
> Finding a new job after getting fired can be hard enough, but Edward F. Wilson never expected the death threats. Wilson, a computer software engineer fired narly a year ago from a small Hawthorne-based aerospace company, says he's paying the price for speaking out against government contracting abuses. The threats -- anonymous, of course -- have come over the telephone twice in recent weeks at his Long Beach home... "Whistleblowing, I'm afraid, is not very popular," he said with a sigh.
>
> He said that soon after being asked ... to draw up software quality-assurance programs required by the government, he realized that Amex Systems officials were doing it strictly for show. "They said to me on several occasions that they had no intention of implementing them," he said.

The article goes on to document Wilson's memo to his employer, his being fired for "being a troublemaker", his filing a wrongful discharge suit, the ensuing criminal investigation currently underway on unnamed government programs, various denials, etc. Dina Rasor, director of the Project on Military Procurement, a self-styled watchdog agency in Washington D.C. spoke about the situation:

> "I've heard of whistleblowers being blackballed from the industry and of government whistleblowers put in 'do-nothing' jobs, but in five years of working with these people I've never had anyone receive a death threat. ... What I've found is so unusual about Ed Wilson is that he made his complaints known to the company well before he was fired. He hasn't brought all this up later as sour grapes."
>
> Wilson said he remains optimistic he will eventually find a job, but admits his "faith in the system is diminishing." "I did what I thought was in the best interests of the country," he said.

Collegiate jungle

Mike McLaughlin <mikemcl@nrl-csr>
Tue, 27 May 86 08:42:00 edt

Darwinian selection will solve the backup problem on campus. Them that backs up will survive, them that don't, won't.

Permission is granted to delete "campus" and insert any other sphere of computer-supported activity presently known or yet to be discovered.

Mike McLaughlin <mikemcl@nrl-csr.arpa>

Decease and Desist -- Death by Computer

Deborah L. Estrin <estrin%usc-cseb@usc-cse.usc.edu>
Mon, 26 May 86 18:43:45 pdt

An editorial appeared in yesterday's (Saturday's) LA Times. It is written by Forman Brown, on the subject of computer error.

Following are a few exerpts:

> "I first became aware of my death last May when my checks began to bounce. Never having experienced bouncing checks before, and knowing that I had quite a respectable balance at the bank, I was both shocked and angry. When I examined the returned checks and found, stamped over my signature on each of them, in red ink, "Deceased", I was mystified. Then, when one of the recipients of my checks, a utility company, demanded that I appear in person, cash in hand, plus $10 for their trouble--their trouble--I was shocked, angry and mystified. I wondered just how they expected us deceased to acquiesce."

Well, to paraphrase, Brown went to the bank, the series of tellers could not believe such a thing had happened and said it was probably the computer's fault and sent him home to write new checks and explanations--including one to a friend who thought he was dead due to the "deceased" notice on the bounced check.

Then the next month he found that his social security payment was not credited to his account. On investigation he found that whatever troubled the computers "had spread to those of the Social Security system as well." This went on for a couple of months despite visits to Social Security. Then finally the bank agreed to credit the amount to his account until Social Security started payment again--which they did several months later.

Brown thought the story was over until his physician contacted him recently to say that Medicare had refused to accept his bill for services rendered becuase the date of the service was six months later than the date of the patient's decease...

He concludes by saying that if he were 20, all this might merely be irritating, but since he is 85 the prospect of death is too near to be treated lightly.

The Death of the Gossamer Time Traveler

Peter G. Neumann <Neumann@SRI-CSL.ARPA>
Wed 28 May 86 22:08:47-PDT

Dr. Paul MacCready has had some marvelous successes, including the first and only human-powered flight across the English Channel in 1979 on his Gossamer Condor. His Time Traveler, a short-winged model of the prehistoric Quetzalcoatlus northropi from 65 million years ago, had made something like 43 consecutive safe flights and starred in a film, "On the Wing", replicating the original appearance and flying style of QN. Weighing in at 44 pounds, it includes battery-operated motors, a computerized autopilot, and ground-based radio controls. Unfortunately, the bird chose the day of its first public appearance, 17 May 86 at Andrews Air Force Base, to have its head break off. Computer archaeologists of the future will of course try to ascertain whether the accident was due to human error in overtaxing the creature, or to a computer program bug in the safety controls that might have otherwise have prevented flight instability, or some other cause. We hope that the head crash can be repaired. The construction cost, variously reported as $500,000 and $700,000, was funded by the National Air and Space Museum and the Johnson Wax Company. [Maybe this was inspired by its more modern precursor, the "one-SEATER WAX-WING".]

Your roving [raving or raven'?] reporter, PGN

Computer Ethics

<rti-sel!dg_rtp!rtp41!dg_rama!bruces%mcnc.csnet@CSNET-RELAY.ARPA>
Tue, 27 May 86 13:36:39 edt

The following is a copy of a review I wrote for a recent newsletter of the Boston chapter of Computer Professionals for Social Responsibility (CPSR). Readers of RISKS may be interested, as well.

METAPHILOSOPHY is a British journal published three times yearly which is dedicated to considerations about particular schools, fields, and methods of philosophy. The October 1985 issue, Computers & Ethics (Volume No. 16, Issue No. 4), is recommended reading [...].

This issue's articles attempt to define and delimit the scope of Computer Ethics, and examine several emerging and current concerns within the field.

One current concern is responsibility for computer-based errors. In his article on the subject, John W. Snapper asks: "...whether it is advisable to ...write the law so that a machine is held legally liable for harm." The author invokes Aristotle's "Nichomachean Ethics" (!) in an analysis of how computers make decisions, and what is meant by "decision" in this context.

On the same subject, William Bechtel goes one step further, considering the possibility that computers could one day bear not only legal, but moral responsibility for decision-making: "When we have computer systems that ...can be embedded in an environment and adapt their responses to that environment, then it would seem that we have captured all those features of human beings that we take into account when we hold them responsible."

Deborah G. Johnson discusses another concern: ownership of computer programs. In "Should Computer Programs Be Owned?," Ms. Johnson criticizes utilitarian arguments for ownership, as well as arguments based upon Locke's labor theory of property. The proper limits to extant legal protections, including copyrights, patents, and trade secrecy laws, are called into question.

Other emerging concerns include the need to educate the public on the dangers and abuses of computers, and the role of computers in education. To this end, Philip A. Pecorino and Walter Maner present a proposal for a college level course in Computer Ethics, and Marvin J. Croy addresses the ethics of computer-assisted instruction.

Dan Lloyd, in his provocative but highly speculative article, "Frankenstein's Children," envisions a world where cognitive simulation AI succeeds in producing machine consciousness, resulting in a possible ethical clash of the rights of artificial minds with human values.

The introductory article, James H. Moor's "What is Computer Ethics," is an ambitious attempt to define Computer Ethics, and to explain its importance. According to Moor, the development and proliferation of computers can rightly be termed "revolutionary": "The revolutionary feature of computers is their logical malleability. Logical malleability assures the enormous application of computer technology." Moor goes on to assert that the Computer Revolution, like the Industrial Revolution, will transform "many of our human activities and social institutions," and will "leave us with policy and conceptual vacuums about how to use computer technology."

An important danger inherent in computers is what Moor calls "the invisibility factor." In his own words: "One may be quite knowledgeable about the inputs and outputs of a computer and only dimly aware of the internal processing." These hidden internal operations can be intentionally employed for unethical purposes; what Moor calls "Invisible abuse," or can contain "Invisible programming values": value judgments of the programmer that reside, insidious and unseen, in the program.

Finally, in the appendix, "Artificial Intelligence, Biology, and Intentional States," editor Terrell Ward Bynum argues against the concept that "intentional states" (i.e. belief, desire, expectation) are causally dependent upon biochemistry, and thus cannot exist within a machine.

If you're at all like me, you probably find reading philosophy can be "tough going," and METAPHILOSOPHY is no exception. References to unfamiliar works, and the use of unfamiliar terms occasionally necessitated my reading passages several times before extracting any meaning from them. The topics, however, are quite relevant and their treatment is, for the most part, lively and interesting. With its well-written introductory article, diverse survey of current concerns, and fairly extensive bibliography, this issue of METAPHILOSOPHY is an excellent first source for those new to the field of Computer Ethics.

[METAPHILOSOPHY, c/o Expediters of the Printed Word Ltd., 515 Madison Avenue, Suite 1217, New York, NY 10022]

Bruce A. Sesnovich   mcnc!rti-sel!dg_rtp!sesnovich
Data General Corp.   rti-sel!dg_rtp!sesnovich%mcnc@csnet-relay.arpa
Westboro, MA   "Problems worthy of attack
                            prove their worth by hitting back"

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 2: Issue 56

Friday, 30 May 1986

Contents

A joke that went wrong

Brian Randell <brian%kelpie.newcastle.ac.uk@Cs.Ucl.AC.UK>
Thu, 29 May 86 10:48:45 bst

From the Guardian (London) 29 May 1985:
ELECTRONIC GOODBYE SHOCKS JOKER
by John Ezard

Mr Dean Talboy's attempt to leave a harmless electronic memento for his former workmates earned him instead a high place in the almanac of computer horror stories, a court was told yesterday.

News of his little prank, and its dire results for the High Street electronics giant Dixons, sent a frisson of sympathy through computer buffs. These are often as tempted by practical jokes as he was. But they also know, as his experience confirms, that one mistyped symbol in a long programme can introduce a monstrous bug into the entire machine.

Mr. Talboys, aged 26, a highly-educated computer consultant, admitted criminal damage at Acton crown court in the first British prosecution for electronic graffiti. His farewell slogan was the innocuous "Goodbye, folks".

Mr. Austen Issard-Davies, prosecuting, said he intended that this should flash up on Dixon's head office computer screen whenever his leaving date was entered by an operator.

But Mr. Talboys inadvertently inserted a "stop" code in his programme, causing the programme to disconnect midway through its run.

Mr. Talboys was crafting his masterpiece while the computer was in test mode. But the machine then transferred it into "production" or operational mode - in which the "stop" symbol is illegal. The outcome of his error was that every screen - in a headquarters which processes the work of 4,500 employees - hiccuped and went blank whenever any operator keyed in anyone's leaving date.

"Unlike most graffiti, which can be rubbed out or painted over, it cost Dixons more than (Pounds)1,000 to investigate, discover what he had done and put it right," Mr Issard-Davies told the court.

The blame was immediately traced to Mr Talboys - "rather like a burglar who has left his visiting card". He had agreed with police that he had acted irresponsibly. Yesterday he was conditionally bound over and ordered to pay the firm (Pounds)1,000 compensation.

The computer language in which Mr Talboys accidentally wrote his bug is called Mantis.

Judge Kerry Quarren-Evans said: "Offices without a certain amount of humour would be very dry and dusty places. But this is not the type of medium for practical jokes."

Mr Talboys said: "My advice to anyone else is don't bloody do it. It has been 18 months of hell. It was simply a prank and I have learned my lesson. My backside has been well and truly tanned."

[I guess we'll be praying mantis will eat more bugs in the future. PGN]

Computer Program for nuclear reactor accidents

Gary Chapman <chapman@su-russell.arpa>
Thu, 29 May 86 11:48:19 pdt

An article in the new Electronics Magazine (McGraw-Hill) May 26, page 14, describes a prototype parallel computer system that would simulate and analyze the chain of events in a complex nuclear accident faster than the accident would actually occur. The system, which is being developed at the University of Illinois Champaign-Urbana campus would combine the power of a parallel processor, with an artifical intelligence/expert system that would examine where a problem is headed and give advice on possible corrections to avoid a disaster. The program does both forward and backward chaining, and is written in Portable Standard Lisp. The system would take inputs from over 1000 sensors on an operating reactor and perform a real-time simulation of the reactor operation. According to the calculations, this package will be able to simulate a reactor accident 10 times faster than real time. The programmer stresses that the system is designed as a monitoring mechanism and decision aid for a human operators, not as an automatic control system.

On risks and knowledge

Alan Wexelblat <wex@mcc.arpa>
Fri, 30 May 86 21:02:10 CDT

One topic so far untouched by RISKS is the intimate connection between risks and knowledge. That is, how can we expect to assess risks when we lack knowledge or worse, when knowledge is deliberately withheld. These thoughts were prompted by the article below:

From "The Guardian", May 21, 1986 (NY, not UK) by Jonathan A. Bennet

The presidentially-appointed Rogers Commission dramatically denounced solid rocket booster manager Lawrence Mulloy, while continuing to conceal multiple cases of perjury by top NASA officials and NASA-White House complicity in that perjury.

The Rogers Commission stopped far short of accusing Mulloy or anyone else of perjury, despite clear contradictions between what its investigators have learned and repeated statements under oath by NASA officials. Instead, the commission merely accused Mulloy of having "almost covered up" and of "glossing over" the truth.

... [I have excerpted the first few paragraphs from a longish message which is sufficiently important to RISKS to be called to your attention, but which is sufficiently non-computer-specific that I did not want to include it in its entirety. It is available for FTPing from SRI-CSL:<RISKS>RISKS-2.56WEX for those of you who can get to it. (Perhaps it can be found in ARMS-D. See next message!) PGN]

Technical vs. Political in SDI

Dave Benson <benson%wsu.csnet@CSNET-RELAY.ARPA>
Thu, 29 May 86 20:38:48 pdt

A while back a RISKS contribution plaintively stated something to the effect that SDI issues were strictly for experts. Not so. There are two somewhat separable matters, the technical (Can SDI be done at acceptable risk/cost) and political (Do we want it anyway? Does it improve security, etc.).

Now RISKS is a place to consider, well, computer risks. Thus it seems appropriate here to explore SDI software issues. The strictly political/ policy issues are on ARMS-D. Since the two aspects of SDI are not entirely separable, some overlap is going to occur.

The contributor of the above mentioned note might like to read msg 787 on ARMS-D from crummer.

Are SDI Software predictions biased by old tactical software?

<estell@nwc-143b>
30 May 86 10:09:00 PST

I'd like to offer an minority opinion about SDI software; i.e., I infer that most RISKS readers agree with the assessments that "... SDI will never be made to work..." At some personal risk, let me say at the outset that SDI, as ballyhooed in the popular press, may never work - certainly not in this decade. But I believe that our projections of the future are inextricably linked to our past. So let me share some observations on Navy tactical software as of 1979.

Much of the OLDER tactical software:
 Was written in assembly language, or CMS-2. Powerful languages like
   FORTRAN and C were not used.
 Was implemented by people who may not have ever sailed or flown in combat.
 Was not well defined functionally by the end users, for lack of "rapid
   prototyping" tools.
 Was written before modern notions like "structured programming" were used.
 Was "shoehorned" into very old, small, slow, unsophisticated computers
   (no hardware floating point, no virtual memory, 4 microsecond cycle).
 "Froze" the modules, instead of the interfaces.

Carriers ran tactical software on machines built of early 1960's technology (germanium diodes). They were remarkable computers for that era, having almost the power of an IBM 7090 in a refrigerator sized box. They severely restricted software development. If replaced, tactical software could be written in several languages, not only Ada (DoD's choice), but also FORTRAN, BASIC, Pascal, C, etc.; the goal is to use standard languages appropriate to the task; and to incorporate modules, and support libraries, already developed and debugged elsewehere.

Turning now to the more common arguments, they seem to be:
(1) COMPLEXITY; i.e., there are too many logical paths through the code;
(2) HISTORY; i.e., no deployed CCCI program has ever worked the first time.

The complexity argument leads one to wonder HOW the human brain works. It has trillions of cells; each has a probability of failure. Some failures are obvious: we forget, we misunderstand, we misspeak; etc. But, inspite of these failures - or because of them - we SATISFICE. Even when some go bonkers, the rest of us try to maintain our sanity. Similarly, one errant SDI computer need not fail the entire network - anymore than one failing IMP need crash the entire ARPANET.

The historical argument leads to an analogy. Suppose that after World War II, President Truman had asked Congress for an R&D program in medicine, to treat many of the physical wounds of the war. Doctors would have pointed out that lost limbs and organs were lost, period. But the progress in the last 25 years changed that. Microsurgery, new drugs, artificial joints, computer assists, including one system that bridged a damaged spinal cord, reinterpreting nerve signals so that a paraplegic could walk again.

The "complexity" and "historical" arguments even interact.
Peter Denning observed years ago that the difficulty of understanding a program is a function of size (among other things). He speculated that difficulty is proportional to the SQUARE of the number of "units of understanding" (about 100 lines of code). Old tactical software, in assembly

language, tends to run into the hundreds of thousands of lines of code; e.g., a 500,000 line program has 5000 units of understanding, with a difficulty index of 25 million. That same program, written in FORTRAN, might shrink to 100,000 lines thus only 1000 units of understanding, thence a difficulty index of one million. That's worth doing!

The medical analogy uncovers another tacit assumption in the SDI argument; neither pro-SDI nor anti-SDI debaters have dealt with it well. It is the "perfection" argument. A missile defense is worth having if it is good enough to save only 5% of the USA population in an all-out nuclear attack. That shield might save 75% of the population in a terrorist attack, launched by an irresponsible source; this is far more likely than a saturation attack by a well armed power like the USSR. As bleak as this prospect is, the facts are that if an all-out attack were launched today, whether by malice, madness or mistake, by either side; and the other side retalliated in full force, the human race would be doomed by fallout, and by nuclear winter.

I am NOT saying that we have the answers within our reach, much less our grasp. I am NOT saying that SDI "as advertised" will be made to work ever, certainly NOT in this decade; I am saying that if we don't try, we won't progress. We know at the outset that SDI will be flawed, though perhaps someday acceptable. That's the status of most of today's high technology; e.g., air traffic control systems, hospitals, electronic banking, telephone systems, mainframe operating systems, ARPANET, ad infinitum.

But my point is that we must not shun the challenge to TRY to improve the software in the field, and the tools used to design and build and test it. That's throwing out the baby with the bathwater! Nor can we extrapolate the successes of the 1990's from the common practices of the 1970's. Rather than deplore the past, we must deploy the technology now developed in Bell Labs, MIT, IBM, Livermore, and other leading computing centers. When I worked in tactical software ('68 - '79), we were about a decade behind the state of the art; e.g., we got high level programming languages, symbolic debuggers, well stocked function libraries, and interactive tools for writing and compiling, in the late '70's; we patterned them on systems at MIT and Berkeley of the late '60's [MULTICS and GENIE].
I wonder just how much of the mid '80's technology is available to tactical developers? Are any tactical computers now offering the architecture and performance of say a CONVEX C-1? Is Prolog available to tactical programmers? Has the "Ada environment" developed the full set of Programmer's Workbench tools that UNIX [tm] offers? and it is widely available?

The disparity between what scientists know MIGHT be done, and what politicians are claiming is a dilemma; how can we pass through its horns?
Tell the SDI proponents in DoD and Congress that:
(1) A perfect shield is a vain wish; and
(2) much progress CAN be made, if RDT&E is done reasonably; and that
(3) the real threat is from terrorists, not Russians.

I think it very likely that we cannot deter SDI, at least not before '89; and even then, Americans will insist on "adequate defense" - even as they complain bitterly about the cost of it. So I suggest that we not try to block SDI, but rather that we refocus its energies and emphases. With luck, we can build a system that will work marginally. It will cost billions; weigh several tons; and consume megawatts of power. In other words, it will be confined to land sites only - not ships, and certainly not space. Thus, it will be fit ONLY for defense. It will be impossible to attack with it. It will become a sort of "Maginot Bubble." Then we could sell the plans to our NATO allies, and to members of the Security Council, including the USSR and China. They won't be able to attack us with them. Perhaps such a demonstration of goodwill would cool the arms race. The longterm economic benefits to the USA are attractive; we could sell systems to nations that wanted them, but couldn't build their own. Some of the revenue could be plowed back into R&D in a many fields, not just defense. The software engineering progress made in behalf of SDI probably would apply immediately to many other computerized systems. Think about it.

Bob

Culling through RISKS headers [ACCIDENTALLY LOST IN RISKS-2.55]

Jim Horning <horning@src.DEC.COM>
Tue, 27 May 86 11:51:06 pdt

[In the message to me that I edited down to nothing in RISKS-2.56 and then added the New York Times excerpts, Jim raised the question of the message headers on RISKS mailings looking rather uninformatively like

53) 16-May RISKS FORUM RISKS-2.53 (10331 chars)

54) 25-May RISKS FORUM RISKS-2.54 (10389 chars)

55) 28-May RISKS FORUM RISKS-2.55 (16307 chars)

and wondering whether anything could be done about it. I responded that I did not see how much useful information could be squirreled away in the message header, but did suggest that a summary of the topics and authors might be useful. So, I think I will simply collect the "CONTENTS:" lines into one issue for each of Vols 1 and 2, and let you do context searches on them. See RISKS-1.46 (NEW!) and RISKS-2.57, respectively, which will be distributed separately. PGN]

Search RISKS using swish-e

Report problems with the web pages to the maintainer