

- Medical Software (Brint Cooper)
- Rolm's Hawk-32 (Doug Bryan)
- Volume 1 Issue 5 (4 Sep 85)
 - The Strategic Defense Initiative (Joseph Weizenbaum)
 - 1.5 million Ford engines need recall? (Hal Murray)
 - Risks in CAD, etc. (Eugene Miya)
 - crt & non-crt risks (Mike McLaughlin)
 - <u>Computerworld... on Union Carbide and NJ false arrests (Charlie Spitzer)</u>
 - More on false arrests (PGN)
- Volume 1 Issue 6 (6 Sep 85)
 - Joseph Weizenbaum's comments (Dave Parnas)
 - Good Risks and Bad Risks (Dave Brandin, PGN)
 - Hot rodding you AT (Dan Bower)
 - Hazards of VDTs and CRTs (Al Friend)
 - <u>crt & non-crt risks (Brint Cooper)</u>
 - The Case of the Broken Buoy (Herb Lin, Matt Bishop)
- Volume 1 Issue 7 (8 Seo 85)
 - The risks of not using some technology (John McCarthy)
 - More on SDI (Joseph Weizenbaum)
 - SDI reliability (Martin Moore)
 - <u>Re: Hazards of VDTs and CRTs (Bernie Elspas)</u>
 - Viruses, Trojan horses, and worms (Fred Hapgood, PGN)
 - Re: The Case of the Broken Buoy (Herb Lin, Matt Bishop)
 - Re: Hot rodding you AT (Keith F. Lynch)

Volume 1 Issue 8 (8 Sep 85)

- Risks of omission (Nancy Leveson, Nicholas Spies, Herb Lin, Dave Parnas)
- Hot rodding you AT and the weather (John McCarthy)
- Re: Good Risks and Bad Risks (Brint Cooper)
- SDI reliability (Herb Lin)
- Viruses, Trojan horses, and worms (Lin and Neumann, 2 each -- his own?)
- Volume 1 Issue 9 (9 Sep 85)
 - McCarthy, Weizenbaum on SDI (Douglas Schuler)
 - Why I'm against even a reliable SDI (Jeffrey Mogul)
 - <u>Risk Assessment and Risk Management (Edward V. Berard)</u>
 - <u>Risks in displaying a file containing control characters (Keith F. Lynch)</u>
- Volume 1 Issue 10 (12 Sep 85)
 - Weizenbaum, etc.; even if SDI worked.... (John Shore)
 - SDI (John McCarthy)
 - More on SDI reliability (Martin Moore)
- Volume 1 Issue 11 (13 Sep 85)
 - SDI and John McCarthy (Charlie Crummer)
 - <u>SDI and Safeguard (John Mashey)</u>
 - SDI and Robert Jastrow (Herb Lin)

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)
- <u>Preserving rights to Email messages (Larry Hunter)</u>
- Risk Comparisons (T. Tussing)
- <u>Risks history/philosophy (Nicholas Spies) [long but interesting]</u>
- 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)
- <u>Mailer Protocol Woes (Marty Moore)</u>
- <u>Another Horror Story -- Sidereal Time Rollover (Marty Moore)</u>
- 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)
 - <u>Re: Moral vs. Technological Progress (Joel Upchurch)</u>
 - <u>Risk Contingency Planning -- Computers in Mexico (Mike McLaughlin)</u>

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)
 - <u>The Mythical Man-Month of Risk (Stavros Macrakis)</u>
 - <u>Risk Assessment by real people (Mike McLaughlin)</u>

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)
 - <u>Computer databases (Andy Mondore)</u>
 - 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)
 - <u>Re: Computer databases (Matt Bishop)</u>
 - 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)
 - <u>Robots are different (Jerry Saltzer)</u>
 - <u>Automobile computer control systems (Bennett Smith)</u>
 - 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)
 - <u>Electromagnetic Interference (Peter G. Neumann)</u>
 - 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)
 - <u>Contents: SPECIAL ISSUE on viruses and worms</u>
- Volume 1 Issue 28 (9 Dec 85)
 - Viruses and Worms (Mark S. Day, Aaron M. Ellison, Ted Lee, Dave Parnas)
 - <u>Electromagnetic Interference (Chuq Von Rospach)</u>
 - <u>Crackers (Peter Reiher, Matt Bishop, Dave Dyer)</u>
- 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)
 - <u>Risks re computer-compared prescriptions (Brint Cooper)</u>
 - <u>Oops (Marty Moore)</u>
 - \$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)
 - <u>Pharmacy prescription systems (Normand Lepine)</u>
 - 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 L
 - 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)
 - <u>Multiple redundancy (Henry Spencer)</u>
 - 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)
 - <u>Multiple redundancy (Henry Spencer)</u>
 - <u>COMPASS 86: System Integrity: Process Security and Safety (Al Friend)</u>
- 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 <u>report</u> any website or feed problems you find to the <u>website maintainer</u>. Report issues with the digest content to the moderator.

Selectors for locating a particular issue from a volume

Volume number: Issue Number:

Volume Index

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

Index to the RISKS Digest

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

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



WELCOME TO RISKS@SRI-CSL

Peter G. Neumann <Neumann@SRI-CSLA.ARPA>

This is the first issue of a new on-line forum. Its intent is to address issues involving risks to the public in the use of computers. As such, it is necessarily concerned with whether/how critical requirements for human safety, reliability, fault tolerance, security, privacy, integrity, and guaranteed service (among others) can be met (in some cases all at the

same time), and how the attempted fulfillment or ignorance of those requirements may imply risks to the public. We will presumably explore both deficiencies in existing systems and techniques for developing better computer systems -- as well as the implications of using computer systems in highly critical environments.

Introductory Comments

This forum is inspired by the letter from Adele Goldberg, President of the Association for Computing Machinery (ACM), in the Communications of the ACM, February 1985 (pp. 131-133). In that message (part of which is reproduced below), Adele outlined the ACM's intensified concern with our increasingly critical dependence on the use of computers, a concern which culminated in the ACM's support for a Forum on Risks to the Public in Computer Systems (RPCS), to be developed by the ACM Committee on Computers and Public Policy (of which I am currently the Chairman). My involvement in this BBOARD activity is thus motivated by my ACM roles, but also by strong feelings that this topic is one of the most important confronting us. In keeping with ACM policy, and with due respect to the use of the ARPANET, we hope to attain a representative balance among differing viewpoints, although this clearly cannot be achieved locally within each instance of the forum.

For discussions on requirements, design, and evaluation techniques for critical systems -- namely, how to do it right in the first place so that a system can satisfy its requirements and can continue to maintain its desired abilities through ongoing maintenance and evolution, you will find a little solace in the literature on computer science, computer systems, and software engineering. There is even some modest encouragement from the formal verification community -- which readers of the ACM SIGSOFT Software Engineering Notes will find in the forthcoming August 1985 special issue on the verification workshop VERkshop III. However, it is not encouraging to find many developers of critical software ignoring what is known about how to do it better. In this RISKS forum, we hope that we will be able to confront some of those problems, and specifically those where risks to the public are present.

You should also be aware (if you are not already) of several related on-line services: HUMAN-NETS@RUTGERS for a variety of issues pertaining to people (but originally oriented to the establishment of WorldNet), SOFT-ENG@MIT-XX for software engineering, and perhaps SECURITY@RUTGERS for security -- it is still young and rather narrow (car-theft prevention is big at the moment, with a few messages on passwords and forged mail headers). (You can get more inforation from SRI-NIC.ARPA:<NETINFO>INTEREST-GROUPS.TXT.) I look at these regularly, so some cross-fertilization and overlap may be expected. However, the perspective of RISKS seems sufficiently unique to justify the existence of still another interest group!

RISKS Forum Procedures

I hope all this introductory detail does not deter you, but it seems to be worthwhile to set things up cleanly from the beginning. To submit items for distribution, send mail to RISKS@SRI-CSL.ARPA. For all other messages (e.g., list additions or deletions, or administrative complaints), send to RISKS-Request@SRI-CSL.ARPA.

Submissions should relate directly to risks to the public involving computer systems, be reasonably coherent, and have a brief explicit descriptive subject line. Flames, ad hominem attacks, overtly political statements, and other inappropriate material will be rejected. Carefulness, reasonably clear writing, and technical accuracy will be greatly appreciated. Much unnecessary flailing can be avoided with just a little forethought.

Contributions will generally be collected and distributed in digest form rather than singly, as often as appropriate. Subject lines may be edited in order to group messages with similar content. Long messages may have portions of lesser interest deleted (and so marked), and/or may be split across several issues.

Initially we will provide distributions to individuals, but as soon as there are more than a few individuals at any given host, we will expect the establishment of a file <BBOARD>RISKS.TXT or equivalent on that host -- with local option whether or not to forward individual copies. Back issues may be FTPed from SRI-CSL.ARPA:\$lt;RISKS\$gt;RISKS-"vol"."no", where "vol" and "no" are volume and number -- i.e., <u>RISKS-1.1</u> for this issue. But please try to rely on local repositories rather than swamping the gateways, nets, and SRI-CSL.

ACM Council Resolution of 8 October 1984

Peter G. Neumann <Neumann@SRI-CSLA.ARPA>

Following are excerpts from ACM President Adele Goldberg's letter in the Communications of the ACM, February 1985 (pp. 131-133).

On this day [8 October 1984], the ACM Council passed an important resolution. It begins:

Contrary to the myth that computer systems are infallible, in fact computer systems can and do fail. Consequently, the reliability of computer-based systems cannot be taken for granted. This reality applies to all computer-based systems, but it is especially critical for systems whose failure would result in extreme risk to the public. Increasingly, human lives depend upon the reliable operation of systems such as air traffic and high-speed ground transportation control systems, military weapons delivery and defense systems, and health care delivery and diagnostic systems.

The second part of the resolution includes a list of technical questions that should be answered about each computer system. This part states that:

While it is not possible to eliminate computer-based systems failure entirely, we believe that it is possible to reduce risks to the public to reasonable levels. To do so, system developers must better recognize and address the issues of reliability. The public has the right to require that systems are installed only after proper steps have been taken to assure reasonable levels of reliability.

The issues and questions concerning reliability that must be addressed include:

- 1. What risks and questions concerning reliability are involved when the computer system fails?
- 2. What is the reasonable and practical level of reliability to require of the system, and does the system meet this level?
- 3. What techniques were used to estimate and verify the level of reliability?
- 4. Were the estimators and verifiers independent of each other and of those with vested interests in the system?

Adele's letter goes on to motivate the ACM's authorization of a forum on risks to the public in the use of computer systems, of which this is an on-line manifestation. As you can see, I believe that the charter must be broader than just reliability, including as appropriate other critical requirements such as fault tolerance, security, privacy, integrity, guaranteed service, human safety, and even world survival (in sort of increasing order of globality). There is also an important but probably sharply delimited role for design verification (such as has been carried out in the multilevel-security community in demonstrating that formal specifications are consistent with formal requirements) and even code verification (proving consistency of code and specifications), although formal verification technologies seem not suited to mammoth systems but only to selected critical components -- assuming that those components can be isolated (which is the operative assumption in the case of security kernels and trusted computing bases). For example, see the VERkshop III proceedings noted above. PGN

AN AGENDA FOR THE FUTURE

Peter G. Neumann <Neumann@SRI-CSLA.ARPA>

One of the activities of the ACM Committee on Computers and Public Policy will be the review of a problem list presented by Dan McCracken and his committee in the September 1974 issue of the Communications of the ACM, and an update of it in the light of dramatic changes in the use of computers since then. Three items from that problem list are particularly relevant to our RISK forum.

- * Computers and money
- * Computers and privacy
- * Computers and elections

Indeed, in the latest issue of the ACM SIGSOFT Software Engineering Notes (July 1985), I reported on a variety of recent money problems, security problems, and a whole string of potential election-fraud problems -- in the last case suggesting opportunities for Trojan Horses and local fraud. On the third subject, there was an article by David Burnham (NY Times) in newspapers of 29 July 1985 (NY Times, SF Chron, etc.), on vulnerabilities in various computerized voting systems. About 60% of the votes are counted by computer programs, with over a third of those votes being counted by one program (or variants?) written by Computer Election Systems of Berkeley CA. Burnham writes, "The allegations that vote tallies calculated with [that program] may have been secretly altered have raised concern among election officials and computer experts... In Indiana and West Virginia, the company has been accused of helping to rig elections." This topic is just warming up.

Items that also give us opportunities for discussions on risks to the public include these:

- * Computers and defense
- * Computers and human safety
- * Computer-user consumer protection
- * Computers and health
- * Informal and formal models of critical properties (e.g., not just of security or reliability, not
- so high-level as Asimov's 3 Laws of Robotics)

Several items on computers and defense are included below. There are also some comments on software that is safe for humans.

I would think that some sort of Ralph-Nader-like consumer protection

organization might be appropriate for computing. We have already had two very serious automobile recalls due to program bugs -- the El Dorado brake computer and the Mark VII computerized air suspension, and at least two heart pacemaker problems (one which resulted in a death), as noted in the disaster list below -- to go along with this summer's watermelon recall (pesticides) and Austrian wine recalls (with the antifreeze-component diethylene glycol being used as a sweetener).

COMPUTER-RELATED INCIDENTS ILLUSTRATING RISKS TO THE PUBLIC

Peter G. Neumann <Neumann@SRI-CSLA.ARPA>

Readers of the ACM SIGSOFT Software Engineering Notes have been alerted in many past issues to numerous disasters and computer curiosities implying potential or actual risks to the public. A summary of events is catalogued below, and updates earlier versions that I circulated in a few selected BBOARDS. Further details can be found in the references cited. Awareness of these cases is vital to those involved the design, implementation, and operation of computer systems in critical environments, but is of course not sufficient to prevent new disasters from occurring. Significantly better systems, and more aware operation and use, are also required.

SOME COMPUTER-RELATED DISASTERS AND OTHER EGREGIOUS HORRORS Compiled by Peter G. Neumann (21 July 1985)

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 10 = 1985. Some incidents are well documented, others need further study. Please send corrections/additions+refs to PGNeumann, SRI International, EL301, 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

------ SYSTEM + ENVIRONMENT ------

- IS Arthritis-therapy microwaves set pacemaker to 214, killed patient (SEN 5 1)
- *S Failed heart-shocking devices due to faulty battery packs (SEN 10 3)
- *S Anti-theft device reset pacemaker; FDA investigating the problem (SEN 10 2)
- *\$ Three Mile Island PA, now recognized as very close to meltdown (SEN 4 2)
- *\$ Crystal River FL reactor (Feb 1980) (Science 207 3/28/80 1445-48, SEN 10 3)
- ** 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) \$S Debit card copying easy despite encryption (DC Metro, SF BART, etc.) \$\$ Microwave phone calls easily interceptable; portable phones spoofable ------ SOFTWARE ------*\$ 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) * 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 cost USA interest on at least 1,150,000 refunds (SEN 10 3) *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) *\$ Colorado River flooding in 1983, due to faulty weather data and/or faulty model; too much water was kept dammed prior to spring thaws. 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) \$ 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] \$ 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) ------ HARDWARE/SOFTWARE ------! Michigan man killed by robotic die-casting machinery (SEN 10 2) ! 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 after he built a newer one. "Jealous Computer Zaps its Creator"! (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) - 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 after computer error led to a 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) \$ A: \$500,000 transaction became \$500,000,000; B: \$200,000,000 lost (SEN 10 3) * FAA Air Traffic Control: many near-misses not reported (SEN 10 3) ------ 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

[See also anecdotes from ACM Symposium on Operating Systems Principles, SOSP 7 (SEN 5 1) and follow-on (SEN 7 1).]

[New Scientist, vol 97, page 502, 24 Feb 83]. Rather, sinking abetted by defensive equipment being turned off to reduce communication interference?

**** DEFENSE COMPUTING SYSTEMS ****

× STRATEGIC COMPUTING INITIATIVE (SCI)

The Strategic Computing Initiative has received considerable discussion in the Communications of the ACM lately, including a letter by Severo Ornstein, Brian Smith and Lucy Suchman (ACM Forum February 1985), the response to them by Robert S. Cooper (ACM Forum, March 1985), and the three responses to Cooper in the August 1985 issue, as well as an article by Mark Stefik in the July 1985 Communications. Considerable variety of opinion is represented, and is well worth reading. PGN

✓ STRATEGIC DEFENSE INITIATIVE (SDI)

The Strategic Defense Initiative (popularly known as Star Wars) is considering the feasibility of developing what is probably the most complex and most critical system ever contemplated. It is highly appropriate to consider the

computer system aspects of that effort here. Some of the potential controversy is illustrated by the recent statements of David Parnas, who presents a strongly skeptical view. (See below.) I hope that we will be able to have a constructive dialogue here among representatives of the different viewpoints, and firmly believe that it is vital to the survival of our world that the computer-technical issues be thoroughly discussed. As in many other cases (e.g., space technology) there are many potential research advances that can spin off approaches to other problems. As indicated by my disaster list above, the problems of developing software for critical environments are very pervasive -- and not just limited to strategic defense. But what we learn in discussing the feasibility of the strategic defense initiative could have great impact on the uses that computers find in other critical environments. In general, we may find that the risks are far too high in many of the critical computing environments on which we depend. We may also be led to techniques for developing better systems that can adequately satisfy all of their critical requirements -- and continue to do so. But perhaps most important of all is the increased awareness that can come from intelligent discussion. Thus, an open forum on this subject is very important. PGN

Mews Item: David Parnas Resigns from SDI Panel

Ed Frankenberry <ezf@bbnccv> 12 Jul 85 13:56:29 EDT (Fri)

Plucked from SOFT-ENG@MIT-XX:

New York Times, 7/12/85, page A6:

SCIENTIST QUITS ANTIMISSILE PANEL, SAYING TASK IS IMPOSSIBLE

By Charles Mohr special to the New York Times

Washington, July 11 - A computer scientist has resigned from an advisory panel on antimissile defense, asserting that it will never be possible to program a vast complex of battle management computers reliably or to assume they will work when confronted with a salvo of nuclear missiles.

The scientist, David L. Parnas, a professor at the University of Victoria in Victoria, British Columbia, who is consultant to the Office of Naval Research in Washington, was one of nine scientists asked by the Strategic Defense Initiative Office to serve at \$1,000 a day on the "panel on computing in support of battle management".

Professor Parnas, an American citizen with secret military clearances, said in a letter of resignation and 17 accompanying memorandums that it would never be possible to test realistically the large array of computers that would link and control a system of sensors, antimissile weapons, guidance and aiming devices, and battle management stations.

Nor, he protested, would it be possible to follow orthodox computer program-writing practices in which errors and "bugs" are detected and eliminated in prolonged everyday use. ...

"I believe," Professor Parnas said, "that it is our duty, as scientists and engineers, to reply that we have no technological magic that will accomplish that. The President and the public should know that." ...

In his memorandums, the professor put forth detailed explanations of his

doubts. He argued that large-scale programs like that envisioned for the program only became reliable through modifications based on realistic use.

He dismissed as unrealistic the idea that program-writing computers, artificial intelligence or mathematical simulation could solve the problem.

Some other scientists have recently expressed public doubts that large-scale programs free of fatal flaws can be written. Herbert Lin, a research fellow at the Massachusetts Institute of Technology, said this month that the basic lesson was that "no program works right the first time."

Professor Parnas wrote that he was sure other experts would disagree with him. But he said many regard the program as a "pot of gold" for research funds or an interesting challenge.

[The above article is not altogether accurate, but gives a flavor of the Parnas position. The arguments for and against feasibility of success need detailed and patient discussion, and thus I do not try to expand upon either pro or con here at this time. However, it is hoped that a serious discussion can unfold on this subject. (SOFT-ENG@MIT-XX vol 1 no 29 provides some further material on-line.) See the following message as well. PGN]

✓ Obtaining Parnas' SDI critique

David Weiss <weiss%wang-inst.csnet@csnet-relay.arpa> Mon 22 Jul 1985 16:09:48 EST

Those who are interested in obtaining copies of David Parnas' technical critique of SDI may do so by writing to the following address:

Dr. David L. Parnas, Department of Computer Science, University of Victoria, P.O. Box 1700, Victoria B.C. V8W 2Y2 CANADA

🗡 BMD paper

Herb Lin <LIN@MIT-MC.ARPA> Mon, 29 Jul 85 16:53:26 EDT

The final version of my BMD paper is available now.

"Software for Ballistic Missile Defense"

Herb Lin, Center for International Studies, 292 Main Street, E38-616, MIT, Cambridge, MA 02142, phone 617-253-8076. Cost including postage = \$4.50

Software for Ballistic Missile Defense, June 1985

Abstract

A battle management system for comprehensive ballistic missile defense

must perform with near perfection and extraordinary reliability. It will be complex to an unprecedented degree, untestable in a realistic environment, and provide minimal time for human intervention. The feasibility of designing and developing such a system (requiring upwards of ten million lines of code) is examined in light of the scale of the project, the difficulty of testing the system in order to remove errors, the management effort required, and the interaction of hardware and software difficulties. The conclusion is that software considerations alone would make the feasibility of a "fully reliable" comprehensive defense against ballistic missiles questionable.

IMPORTANT NOTE: this version supersedes a widely circulated but earlier draft entitled "Military Software and BMD: An Insoluble Problem?" dated February 1985.

Minireview of Freeman Dyson's Weapons and Hope

Peter Denning <pjd@RIACS.ARPA> Tuesday 30 Jul 85 17:17:56 pdt

I've just finished reading WEAPONS AND HOPE, by Freeman Dyson, published recently. It is a remarkable book analyzing the tools, people, and concepts used for national defense. The goal is to set forth an agenda for discussing the nuclear weapons problem. The most extraordinary aspect of the book is that Dyson fairly and accurately represents the many points of view with sympathy and empathy for each. He thus transmits the impression that it is possible for everyone to enter into and participate intelligently in this important debate, and he tells us what the fundamental questions we must address are. This book significantly altered the way in which I personally look at the problem. I recommend that everyone read it and that we all use it as a point of departure for our own discussions.

Although Dyson leaves no doubt on his personal views, he presents his very careful arguments and lays out all the reasoning and assumptions where they can be scrutinized by others. With respect to the SDI, Dyson argues (convincingly, I might add) that the greatest risk comes from the interaction of the SDI system with the existing policies of the US and Soviet Union -- it may well destabilize that interaction. His argument is based on policy considerations and is largely insensitive to the question whether an SDI system could meet its technical goals. For other reasons he analyzes at length, he considers the idea of a space defense system to be a technical folly.

Most of the arguments I've seen computer scientists make in criticism of the "star wars" system are technically correct and support the technical-folly view but may miss the point at a policy level. (I am thinking of arguments like

"Computer scientists ought to oppose this because technically it cannot meet its goals at reasonable cost.")

The point is that to the extent that policy planners perceive the technical arguments as being largely inessential at the policy level, they will not

take seriously arguments labelled

"You must take this argument seriously because it is made by computer scientists."

Politicians often argue that is their job to evaluate the spectrum of options, make the moral judgments, and puts risks in their proper place -technologists ought to assess the risks, but when it comes to judging whether those risks are acceptable (a moral or ethical judgment), technologists have no more expertise than, say, politicians. So in a certain important sense, computer scientists have little special expertise to bring to the debate. For this reason, I think ACM has taken the right approach by giving members [and nonmembers! <PGN>] a forum in which to discuss these matters as individual human beings but without obligating ACM to take official positions that are easily dismissed by policy planners as outside ACM's official expertise.

Peter Denning

[In addition, you might want to look at "The Button: The Pentagon Strategic Command and Control System", Simon and Schuster, 1985, which is also a remarkable book. It apparently began as an attempt to examine the survivability of our existing communications and rapidly broadened into a consideration of the computer systems as well. I cite several examples in the catalog above. Some of you probably saw excerpts in the New Yorker. PGN]

Responsible Use of Computers

Jim Horning <horning@decwrl.ARPA> 30 Jul 1985 1149-PDT (Tuesday)

You might want to mention the evening session on "Our Responsibility as Computer Professionals" held in conjunction with TAPSOFT in Berlin, March 27, 1985. This was attended by about 400 people. Organized by R. Burstall, C. Floyd, C.B. Jones, H.-J. Kreowski, B. Mahr, J. Thatcher. Christiane Floyd wrote a nice position paper for the TAPSOFT session, well worth abstracting and providing a reference to.

Jim Horning

[This position paper is apparently similar to an article by Christiane Floyd, "The Responsible Use of Computers -- Where Do We Draw the Line?", that appears in two parts in the Spring and Summer 1985 issues of the CPSR Newsletter (Computer Professionals for Social Responsibility, P.O. Box 717, Palo Alto CA 94301). Perhaps someone can send us the TAPSOFT abstract. PGN]

HUMAN SAFETY (SOFTWARE SAFETY)

Peter G. Neumann <Neumann@SRI-CSL>

An important area of concern to the RISKS forum is what is often called Software Safety, or more properly the necessity for software that is safe for humans. ("Software Safety" could easily be misconstrued to imply making the software safe FROM humans, an ability that is called "integrity" in the security community.) Nancy Leveson has been doing some excellent work on that subject, and I hope she will be a contributor to RISKS. There are also short letters in the ACM Forum from Peter Fenwick (CACM December 1984) and David Nelson (CACM March 1985) on this topic, although they touch only the tip of the iceberg. I would expect human safety to be a vital topic for this RISKS forum, and hope that we can also help to stimulate research on that topic.

INTERNATIONAL SEMINAR ON COMPUTERS IN CRITICAL ENVIRONMENTS

In sticking to my convictions that we must address a variety of critical computing requirements in a highly systematic, unified, and rigorous way, I am involved in the following effort:

23-25 October 1985, Rome, Italy (organized by Sipe Optimation and T&TSUD, sponsored by Banca Nazionale del Lavoro). Italian and English. Organizers Roberto Liscia (Sipe Optimation, Roma, via Silvio d'Amico 40, ITALIA, phone 039-6-5476), Eugenio Corti (T&TSUD, 80127 Napoli, via Tasso 428, ITALIA), Peter G. Neumann (SRI International, Menlo Park CA 94025). Speakers include Neumann, Bill Riddle, Severo Ornstein (CPSR), Alan Borning (U. Washington), Andres Zellweger (FAA), Sandro Bologna (ENEA), Eric Guldentops (SWIFT). The program addresses a broad range of topics (including technical, management, social, and economic issues) on the use of computer systems in critical environments, where the computer systems must be (e.g.) very reliable, fault-tolerant, highly available, secure, and safe for humans. This symposium represents an effort to provide a unified basis for the development of critical systems. Software engineering and the role of the man-machine interface are addressed in detail. There will also be case studies of air-traffic control systems, defense systems, funds transfer, and nuclear power. Contact Roberto Liscia (or Mrs. De Vito) at SIPE, or Peter Neumann at SRI for further information.

🗡 AFTERWORD

Congratulations to you if you made it through this rather lengthy inaugural issue. I hope you find this and subsequent issues provocative, challenging, enlightening, interesting, and entertaining. But that depends in part upon your contributions having those attributes. Now it is in YOUR hands: your contributions and suggestions will be welcomed. PGNeumann <Neumann@SRI-CSL>



Search RISKS using swish-e

Report problems with the web pages to the maintainer



Introduction, and more recent risk items

Peter G. Neumann <Neumann@SRI-CSL> 27 Aug 1985 23:32:01-PST

I was away during the previous three weeks, which made it difficult to put out another issue. However, the newspapers were full of excitement relevant to this forum:

A Federal district judge awarded \$1.25 million to the families of three lobstermen who were lost at sea in a storm that the National Weather Service failed to predict because its parent organization (the National Oceanic and Atmospheric Administration) had not repaired a weather buoy for three months. [NY Times 13 Aug 85]

- Another Union Carbide leak (causing 135 injuries) resulted from a computer program that was not yet
 programmed to recognize aldicarb oxime, compounded by human error when the operator misinterpreted the
 results of the program to imply the presence of methyl isocyanate (as in Bhopal). A 20-minute delay in notifying
 county emergency made things worse. [NY Times 14 and 24 Aug 85 front pages] (There were two other serious
 Union Carbide incidents reported in August as well, although only this one had a computer link.)
- An untimely -- and possibly experiment-aborting -- delay of the intended 25 August launch of the space shuttle Discovery was caused when a malfunction in the backup computer was discovered just 25 minutes before the scheduled launch. The delay threatened to seriously compromise the mission. [NY Times 26 August 1985] The Times reporter John Noble Wilford wrote, "What was puzzling to engineers was that the computer had worked perfectly in tests before today. And in tests after the failure, it worked, though showing signs of trouble." Arnold Aldrich, manager of the shuttle program at Johnson, was quoted as saying "We're about 99.5% sure it's a hardware failure." (The computers are state of the art as of 1972 and are due for upgrading in 1987.) A similar failure of just the backup computer caused a one-day delay in Discovery's maiden launch last summer.
- More details are emerging on possible computer hanky-panky in elections, including the recent Philippine elections. There has been a series of articles in the past weeks by Peter Carey in the San Jose Mercury News -- which I haven't seen yet but will certainly hope to report on.

I expect that future issues of this RISKS forum will appear at a higher frequency -- especially if there is more interaction from our readership. I will certainly try to redistribute appropriate provocative material on a shorter fuse. I hope that we can do more than just recapture and abstract things that appear elsewhere, but that depends on some of you contributing. I will be disappointed (but not surprised) to hear complaints that we present only one side of any particular issue, particularly when no countering positions are available or when none are provoked in response; if you are bothered by only one side being represented, you must help to restore the balance. However, remember that it is often easier to criticize others than to come up with constructive alternatives, and constructive alternatives are at the heart of reducing risks. So, as I said in vol 1 no 1, let us be constructive.

Mariner 1 irony

<Nicholas.Spies@CMU-CS-H.ARPA> 16 Aug 1985 21:23-EST

My late father (Otto R. Spies) was a research scientist at Burroughs when the Mariner 1 launch failed. He brought home an internal memo that was circulated to admonish all employees to be careful in their work to prevent similar disasters in the future. (I don't recall whether Burroughs was directly involved with Mariner 1 or not.) After explaining that a critical program bombed because a period was substituted for a comma, the memo ended with the phrase

"... no detail is to [sic] small to overlook."

My father would be deeply pleased that people who can fully appreciate this small irony are now working on ways to prevent the misapplication of computers as foible-amplifiers.

Forum on Risks to the Public in Computer Systems [Reaction]

_Bob <Carter@RUTGERS.ARPA> 8 Aug 85 19:10 EDT (Thu)

Thanks for the copy of Vol. I, No. 1. Herewith a brief reaction. This is sent to you directly because I'm not sure whether discussion of the digest is appropriate for inclusion in the digest.

1. Please mung RISKS so that it does not break standard undigestifying software (in my case, BABYL).

[BABYL is an EMACS-TECO hack. It seems to be a real bear to use, with lots of pitfalls still. But I'll see what I can do. Alternatively, shorter issues might help. PGN]

2. I think RISKS is clearly an idea whose time has come, but I'm not entirely sure it has been sufficiently thought through.

[I should hope not! It is a cooperative venture. I just happen to be trying to moderate it. PGN]

a. You cast your net altogether too widely, and include some topics that have been discussed extensively on widely-read mailing lists. Star Wars, the Lin paper, the Parnas resignation, and related topics have been constructively discussed on ARMS-D. I have considerable doubt about the utility of replicating this discussion. (The moderators of HUMAN-NETS and POLI-SCI have both adopted the policy of directing SDI debate to that forum. Would it be a good idea to follow that example?

[To some extent, yes. However, one cannot read ALL of the interesting BBOARDs -- there are currently hundreds on the ARPANET alone, many of which have some bearing on RISKS. Also, browsers from other networks are at a huge disadvantage unless they have connections, hours of spare time, money, etc. This is a FORUM ON RISKS, and should properly address that topic. We certainly should not simply reproduce other BBOARDS, but some duplication seems tolerable. (I'll try to keep it at the end of each issue, so you won't have to wade through it.) By the way, I had originally intended to mention ARMS-D in <u>RISKS vol 1 no 1</u>, but did not have time to check it out in detail. For those of you who want to pursue it, next following is the essence of the blurb taken from the Network Information Center, SRI-NIC.ARPA:<NETINFO>INTEREST-GROUPS.TXT. PGN]

[ARMS-D@MIT-MC:

The Arms-Discussion Digest is intended to be a forum for discussion of arms control and weapon system issues. Messages are collected, edited into digests and distributed as the volume of mail dictates (usually twice a week).

Old digests may be FTP'ed from MIT-MC(no login required). They are archived at BALL; ARMSD ARCn , where n is the issue no.

All requests to be added to or deleted from this list, problems, questions, etc., should be sent to Arms-D-REQUEST@MIT-MC.

Moderator: Harold G. Ancell <HGA@MIT-MC>]

b. You do not cover the topics which, in my opinion, are going to generate more law-making than anything you do touch on. In particular, the health hazards (if any) of CRT use, and the working conditions (including automated performance testing) of "pink-collar" CRT users are going to be among the most important labor-relations issues of the next few years. Many people think these more imminent risks than those mentioned in the RISKS prospectus.

[Fine topic! PGN]

3. I think a digest is an animal that differs considerably from print media, but is no less important. I get the feeling that you consider yourself a country cousin of the ACM publications and of SEN. Wrong! You're not inferior, you are just editing in a different medium and as you put your mind to the task, I hope you come to take them with a larger grain of salt. In particular,

! Chinese computer builder electrocuted by his smart computer after he built a newer one. "Jealous Computer Zaps its Creator"! (SEN 10 1)

was a National Inquirer-style joke. The editor of SEN should not have reprinted it, and you probably should not have included it in a serious list of computer-related failures.

[The editor of SEN has sometimes been known to indulge in levity. In this case it appears that a Chinese engineer was indeed electrocuted -- and that is an interesting case of computer-related disaster. On the other hand, if someone can believe that an AI automatic programming routine can write many million lines of correct code, then he might as well believe that a smart computer system could express jealousy and cause the electrocution! Actually, Bob used "PEN" throughout rather than "SEN", but "Software Engineering Notes" was the only sensible interpretation I could come up with, so I changed it. Do I have a "PEN" pal? PGN]

4. It seems to me that it is precisely in the area of serious hardware and software failures that RISKS should make its mark. Directing itself to that topic, it fills a spot no existing list touches on directly, and treats a matter that concerns every computer professional who is earning a decent living. Litigation about defective software design and programming malpractice will be the inevitable consequence of risks, and RISKS is the only place to discuss avoiding them. Please consider focussing the list more closely on that subject.

[Bob, Thanks for your comments. I heartily agree on the importance of the last item. But, I do not intend to generate all of the material for this forum, and can only smile when someone suggests that this forum is not what it should be. I look forward to your help! PGN]

[End of Bob Carter's message and my interspersions.]

KISKS forum [including An Air-Traffic Control Problem]

Scott M. Rose <rose@uw-bluechip.arpa> 16 Aug 85 21:06:39 PDT (Fri)

I had kind of hoped that somebody would submit something on the recent problem in Aurora Illinois, whereby a computer cable was cut that brought information from RADAR sensors to the regional air traffic control center there. Supposedly, the system was designed to be sufficiently redundant to handle such a failure gracefully, but this turned out not to be the case: there were several close calls as the system went up and down repeatedly. There was information about the problem in the New York Times and the Chicago Tribune, at least... but not in very good detail.

I wonder if the forum is the right format for such a group. The problem is that one may find oneself reluctant to report on such an incident that was widely reported in the popular press, and was current, for fear that a dozen others have done the same. Yet in this case, the apparent result is that NOBODY reported on it, and I think such an event ought not pass without note on this group. I might propose something more like the info-nets group, where postings are automatically forwarded to group members. If problems arose, then the postings could be filtered by the moderator... say, on a daily basis? Just an idea...

-S Rose

[Please don't feel reluctant to ask whether someone has reported an interesting event before you go to any potentially duplicate effort. We'd rather not miss out entirely.]

Kisks in AI Diagnostic Aids

<Smith@UDel-Dewey.ARPA> Sun, 18 Aug 85 12:23:25 EDT

I would enjoy a discussion on the legal and ethical problems that have come up with the creation of AI diagnostic aids for doctors. Who takes the blame if the advice of a program causes a wrong diagnosis? The doctor (if so, then who would use such a program!?!?), the program's author(s) (if so, then who would write such a program!?!?), the program (if so, then who would market such a program!?!?), These nagging questions

will have to be answered before anyone is going to make general use of these programs I would be very interested in hearing what other people think about this question. It seems to me that it would be a suitable one for this bboard.

art smith

(smith@UDel-Dewey.ARPA)

Following are several items on the Strategic Defense Initiative and related subjects.

WARNING!! [A Trojan Horse Bites Man]

Don Malpass <malpass@ll-sst> Thu, 15 Aug 85 11:05:48 edt

Today's Wall St. Journal contained the following article. I think it is of enough potential significance that I'll enter the whole thing. In addition to the conclusions it states, it implies something about good backup procedure discipline.

In the hope this may save someone,

Don Malpass

(8/15/85 Wall St. Journal) ARF! ARF!

Richard Streeter's bytes got bitten by an "Arf Arf," which isn't

a dog but a horse.

Mr. Streeter, director of development in the engineering department of CBS Inc. and home-computer buff, was browsing recently through the offerings of Family Ledger, a computer bulletin board that can be used by anybody with a computer and a telephone to swap advice, games or programs or to make mischief. Mr. Streeter loaded into his computer a program that was billed as enhancing his IBM program's graphics; instead it instantly wiped out the 900 accounting, word processing and game programs he had stored in his computer over the years. All that was left was a taunt glowing back at him from the screen: "Arf! Arf! Got You!"

"HACKERS" STRIKE AGAIN

This latest form of computer vandalism - dubbed for obvious reasons a Trojan Horse - is the work of the same kind of anonymous "hackers" who get their kicks stealing sensitive data from government computers or invading school computers to change grades. But instead of stealing, Trojan Horses just destroy all the data files in the computer.

Trojan Horse creators are nearly impossible to catch - they usually provide phony names and addresses with their programs - and the malevolent programs often slip by bulletin-board operators. But they are becoming a real nuisance. Several variations of the "Arf! Arf!" program have made the rounds, including one that poses as a "super-directory" that conveniently places computer files in alphabetical order.

Operators have begun to take names and addresses of electronic bulletin-board users so they can check their authenticity. When a computer vandal is uncovered, the word is passed to other operators. Special testing programs also allow them to study the wording of submitted programs and detect suspicious commands. INTERFACER BEWARE

But while Al Stone, the computer consultant who runs Long Island based Family Ledger, has such a testing program, he says he didn't have time to screen the "Arf! Arf!" that bit Mr. Streeter. "Don't attempt to run something unless you know its pedigree," he says. That's good advice, because the computer pranksters are getting more clever - and nastier. They are now creating even-more-insidious programs that gradually eat away existing files as they are used. Appropriately enough, these new programs are known as "worms".

(8/15/85 Wall St. Journal)

Software engineering and SDI

<mooremj@EGLIN-VAX> Mon, 19 Aug 85 13:56:21 CDT

[FROM Soft-Eng Digest Fri, 23 Aug 85 Volume 1 : Issue 31]

>Dr. David Parnas has quite accurately pointed out some of the dangers inherent in the software to be written for the Strategic Defense Initiative. I must take exception, however, to the following statement from the Boston Globe story quoted in Volume 1, Issue 29, of this digest:

"To imagine that Star Wars systems will work perfectly without testing is ridiculous. A realistic test of the Strategic Defense Initiative would require a practice nuclear war. Perfecting it would require a string of such wars."

There are currently many systems which cannot be fully tested. One example is the software used in our present defense early warning system. Another example, one with which I am personally familiar, is the Range Safety Command Destruct system at Cape Canaveral Air Force Station. This system provides the commands necessary to destroy errant missiles which may threaten populated areas; I wrote most of the software for the central computer in this system. The system can never be fully tested in the sense implied above, for to do so would involve the intentional destruction of a missile for testing purposes only. On the other hand, it must be reliable: a false negative (failure to destroy a missile which endangers a populated area) could cause the loss of thousands of lives; a false positive (unintentional destruction of, say, a Space Shuttle mission) is equally unthinkable. There are many techniques available to produce fault-tolerant, reliable software, just as there are for hardware; the Range Safety system was designed by some of the best people at NASA, the U.S. Air Force, and several contractors. I do not claim that a failure of this system is "impossible", but the risk of a failure, in my opinion, is acceptably low.

"But ANY risk is too great in Star Wars!"

I knew someone would say that, and I can agree with this sentiment. The only alternative, then, is not to build it, because any system at all will involve some risk (however small) of failure; and failure will, as Dr. Parnas has pointed out, lead to the Ultimate Disaster. I believe that this is what Dr. Parnas is hoping to accomplish: persuading the authorities that the risk is unacceptable. It won't work. Oh, perhaps it will in the short run; "Star Wars" may not be built now, or ever. But sooner or later, some system will be given life-and-death authority over the entire planet, whether it is a space defense system, a launch-on-warning strategic defense system, or something else. The readers of this digest are the present and future leaders in the field of software engineering. It is our responsibility to refine the techniques now used and to develop new ones so that these systems WILL be reliable. I fear that some first-rate people may avoid working on such systems because they are "impossible"; this will result in second-rate people working on them, which is something we cannot afford. This is NOT a slur at Dr. Parnas. He has performed an invaluable service by bringing the public's attention to the problem. Now it is up to us to solve that problem.

I apologize for the length of this message. The above views are strictly my own, and do not represent my employer or any government agency.

Martin J. Moore Senior Software Analyst RCA Armament Test Project P. O. Box 1446 Eglin AFB, Florida 32542 ARPAnet: MOOREMJ@EGLIN-VAX.ARPA

Software engineering and SDI

From: horning@decwrl.ARPA (Jim Horning) Date: 21 Aug 1985 1243-PDT (Wednesday) To: Neumann@SRI-CSLA Subject: Trip Report: Computing in Support of Battle Management

[This is a relatively long report, because I haven't been able to come up with a simple characterization of an interesting and informative day.]

Background:

On August 13 I travelled to Marina del Rey to spend a day with the U.S. Department of Defense Strategic Defense Initiative Organization Panel on Computing in Support of Battle Management (DoD SDIO PCSBM).

SDI is the "Star Wars" antiballistic missile system; PCSBM is the panel Dave Parnas resigned from.

I wasn't really sure what to expect. As I told Richard Lau when he invited me to spend a day with them, I'd read what Parnas wrote, but hadn't seen the other side. He replied that the other side hadn't been written yet. "Come on down and talk to us. The one thing that's certain is that what we do will have an impact, whether for good or for ill."

Summary:

The good news is that the panel members are not crazies; they aren't charlatans; they aren't fools. If a solution to SDI's Battle Management

Software problem can be purchased for five billion dollars (or even ten), they'll probably find it; if not, they'll eventually recognize that it can't.

The bad news is that they realize they don't have the expertise to solve the problem themselves, or even to direct its solution. They accept Dave Parnas's assessment that the software contemplated in the "Fletcher Report" cannot be produced by present techniques, and that AI, Automatic Programming, and Program Verification put together won't generate a solution. Thus their invitations to people such as myself, Bob Balzer, and Vic Vyssotsky to come discuss our views of the state and prospects of software technology.

I think a fair summary of the panel's current position is that they are not yet convinced that the problem cannot be modified to make it soluble. ("Suppose we let software concerns drive the system architecture? After all, it is one of the two key technologies.") They are trying to decide what must be done to provide the information that would be needed in the early 1990s to make a decision about deploying a system in the late 1990s.

Assumptions:

Throughout the day's discussions, there were repeated disconnects between their going-in assumptions and mine. In fairness, they tried to understand the sources of the differences, to identify their assumptions, and to get me to identify and justify mine.

* Big budgets: I've never come so close to a trillion-dollar (\$10**12) project before, even in the planning stage. ("The satellite launches alone will cost upwards of \$500 billion, so there's not much point in scrimping elsewhere.")

- I was unprepared for the intensity of their belief that any technical problem could be steamrollered with a budget that size.

- They seemed surprised that I believed that progress in software research is now largely limited by the supply of first-rate people, and that the short-term effect of injecting vastly more dollars would be to slow things down by diverting researchers to administer them.

* Big software: They were surprised by my observation that for every order of magnitude in software size (measured by almost any interesting metric) a new set of problems seems to dominate.

This implies that no collection of experiments with million-line
"prototypes" can ensure success in building a ten-million-line system.
I argued that the only prototype from which they would learn much would be a full-scale, fully-functional one. Such a prototype would also reveal surprising consequences of the specification.
(The FIFTEENTH LAW OF SYSTEMANTICS: A complex system that works is invariably found to have evolved from a simple system that works.)

- Only Chuck Seitz and Bijoy Chatterjee seemed to fully appreciate why

software doesn't just "scale up" (doubtless because of their hardware design experience). It is not a "product" that can be produced at some rate, but the design of a family of computations; it is the computations that can be easily scaled.

* Reliability: I had assumed that one of the reasons Battle Management software would be more difficult than commercial software was its more stringent reliability requirement. They assume that this is one of the parameters that can be varied to make the problem easier.

Discussion:

The Panel is still in the process of drafting its report on Battle Management Systems. Although they take the need to produce such a system as a given, almost anything else is negotiable. (In particular, they do not accept the "Fletcher Report" as anything more than a springboard for discussion, and criticize current work for following it too slavishly. The work at Rome Air Development Center--which produced estimates like 24.61 megalines of code, 18.28 gigaflops per weapons platform--was mentioned contemptuously, while the Army work at Huntsville was considered beneath contempt.)

The following comments are included merely to indicate the range and diversity of opinions expressed. They are certainly not official positions of the panel, and--after being filtered though my understanding and memory--may not even be what the speaker intended. Many of the inconsistencies are real; the panel is working to identify and resolve them.

- The problem may be easier than a banking system, because: each autonomous unit can be almost stateless; a simple kernel can monitor the system and reboot whenever a problem is detected; there are fewer people in the loop; more hardware overcapacity can be included.

- If you lose a state it will take only a few moments to build a new state. (Tracks that are more than 30 minutes old are not interesting.)

- Certain kinds of reliability aren't needed, because: a real battle would last only a few minutes; the system would be used at most once; with enough redundancy it's OK for individual weapons to fail; the system doesn't have to actually work, just be a credible deterrent; the system wouldn't control nuclear weapons--unless the Teller "pop up" scheme is adopted; the lasers won't penetrate the atmosphere, so even if the system runs amok, the worst it could do would be to intercept some innocent launch or satellite.

- We could debug the software by putting it in orbit five or ten years before the weapons are deployed, and observing it. We wouldn't even have to deploy them until the system was sufficiently reliable. Yes, but this would not test the important modes of the system.

- Dependence on communication can be minimized by distributing authority: each platform can act on its own, and treat all

communication as hints.

- With a multi-level fault-tolerance scheme, each platform can monitor the state of its neighbors, and reboot or download any that seem to be malfunctioning.

- In fifteen years we can put 200 gigaflops in orbit in a teacup. Well, make that a breadbox.

- Space qualification is difficult and slow. Don't count on microprocessors of more than a few mips in orbit. Well, maybe we could use fifty of them.

- How much can we speed up computations by adding processors? With general-purpose processors, probably not much. How much should we rely on special-purpose space-qualified processors?

- Processor cost is negligible. No, it isn't. Compared to software costs or total system costs it is. No, it isn't, you are underestimating the costs of space qualification.

- 14 MeV neutron flux cannot effectively be shielded against and represents a fundamental limitation on the switching-speed, power product. Maybe we should put all the computationally intensive components under a mountain. But that increases the dependence on communication.

- Maybe we could reduce failure rates by putting the software in read-only memory. No, that makes software maintenance incredibly difficult.

- Flaccidware. It's software now, but it can become hardware when necessary.

- Is hardware less prone to failure if switched off? Maybe we could have large parts of the system on standby until the system goes on alert. Unfortunately, the dominant hardware failure modes continue even with power off.

- The software structure must accommodate changes in virtually all component technologies (weapons, sensors, targets, communication, computer hardware) during and following deployment. But we don't have much technology for managing rapid massive changes in large systems.

Relation to Critics:

Dave Parnas's criticisms have obviously been a matter of considerable concern for the panel. Chuck Seitz and Dick Lau both said explicitly that they wouldn't be satisfied making a recommendation that failed to address the issues Dave and other critics have raised. Chuck also distributed copies of "The Star Wars Computer System" by Greg Nelson and David Redell, commending it to the attention of the panel as "Finally, some well-written and intelligent criticism." Richard Lipton had a somewhat different attitude: How can they say that what we are going to propose is impossible, when even we don't know yet what we're going to propose? And why don't software researchers show more imagination? When a few billion dollars are dangled in front of them, the physicists will promise to improve laser output by nine decimal orders of magnitude; computer scientists won't even promise one or two for software production.

The minutes of the August 12 meeting contain the following points:

- Critics represent an unpaid "red team" and serve a useful function in identifying weak points in the program.

- Critiques should be acknowledged, and areas identified as to how we can work to overcome these problem areas.

- Throughout our discussions, and in our report we should reflect the fact that we have accepted a degree of uncertainty as an inherent part of the strategic defense system.

- How to get the system that is desired? This basic problem goes back to defining requirements--a difficult task when one is not quite sure what one wants and what has to be done.

Prospects:

After all of this, what do I think of the prospects for SDI Battle Management Software? I certainly would not be willing to take on responsibility for producing it. On the other hand, I cannot say flatly that no piece of software can be deployed in the 1990s to control a ballistic missile defense system. It all depends on how much functionality, coordination, and reliability are demanded of it.

Unfortunately, as with most other computer systems, the dimension in which the major sacrifice will probably be made is reliability. The reality of the situation is that reliability is less visible before deployment than other system parameters and can be lost by default. It is also probably the hardest to remedy post facto. Of course, with a system intended to be used "at most once," there may be no one around to care whether or not it functioned reliably.

Despite these misgivings, I am glad that this panel is taking seriously its charter to develop the information on which a deployment decision could responsibly be based.

Jim H.

Software engineering and SDI

[An earlier SU-bboard message that prompted the following sequence of replies seemed like total gibberish, so I have omitted it. PGN]

Date: 13 Aug 85 1521 PDT

From: John McCarthy <JMC@SU-AI.ARPA> Subject: Forum on Risks to the Public in Computer Systems To: su-bboards@SU-AI.ARPA [but not To: RISKS...]

I was taking [as?] my model Petr Beckmann's book "The Health Hazards of not Going Nuclear" in which he contrasts the slight risks of nuclear energy with the very large number of deaths resulting from conventional energy sources from, e.g. mining and air pollution. It seemed to me that your announcement was similarly one sided in its consideration in risks of on-line systems and ignoring the possibility of risks from their non-use. I won't be specific at present, but if you or anyone else wants to make the claim that there are no such risks, I'm willing to place a substantial bet.

[Clearly both inaction and non-use can be risky. The first two items at the beginning of this issue (Vol 1 no 2) -- the lobstermen and the Union Carbide case -- involved inaction. PGN]

Software engineering and SDI

Date: 14 Aug 85 1635 PDT From: John McCarthy <JMC@SU-AI.ARPA> Subject: IJCAI as a forum To: su-bboards@SU-AI.ARPA

Like Chris Stuart, I have also contemplated using IJCAI as a forum. My issue concerns the computer scientists who have claimed, in one case "for fundamental computer science reasons" that the computer programs required for the Strategic Defense Initiative (Star Wars) are impossible to write and verify without having a series of nuclear wars for practice. Much of the press (both Science magazine and the New York Times) have assumed (in my opinion correctly) that these people are speaking, not merely as individuals, but in the name of computer science itself. The phrase "for fundamental computer science reasons" was used by one of the computer scientist opponents.

In my opinion these people are claiming an authority they do not possess. There is no accepted body of computer science principles that permits concluding that some particular program that is mathematically possible cannot be written and debugged. To put it more strongly, I don't believe that there is even one published paper purporting to establish such principles. However, I am not familiar with the literature on software engineering.

I think they have allowed themselves to be tempted into exaggerating their authority in order to support the anti-SDI cause, which they support for other reasons.

I have two opportunities to counter them. First, I'm giving a speech in connection with an award I'm receiving. Since I didn't have to submit a paper, I was given carte blanche. Second, I have been asked by the local arrangements people to hold a press conference. I ask for advice on whether I should use either of these opportunities. I can probably even arrange for some journalist to ask my opinion on the Star Wars debugging issue, so I wouldn't have to raise the issue myself. Indeed since my position is increasingly public, I might be asked anyway.

To make things clear, I have no position on the feasibility of SDI, although I hope it can be made to work. Since even the physical principles that will be proposed for the SDI system haven't been determined, it isn't possible to determine what kind of programs will be required and to assess how hard they will be to write and verify. Moreover, it may be possible to develop new techniques involving both simulation and theorem proving relevant to verifying such a program. My sole present point is that no-one can claim the authority of computer science for asserting that the task is impossible or impractical.

There is even potential relevance to AI, since some of the opponents of SDI, and very likely some of the proponents, have suggested that AI techniques might be used.

I look forward to the advice of BBOARD contributors.

Software engineering and SDI

Date: Thu 15 Aug 85 00:17:09-PDT From: Peter Karp <KARP@SUMEX-AIM.ARPA> Subject: Verifying SDI software To: su-bboard@SUMEX-AIM.ARPA

John McCarthy: I argue CPSR's approach is reasonable as follows:

- 1) I assume you admit that bugs in the SDI software would be very bad since this could quite conceivably leave our cities open Soviet attack.
- 2) You concede software verification theory does not permit proof of correctness of such complex programs. I concede this same theory does not show such proofs are impossible.
- 3) The question to responsible computer professionals then becomes: From your experience in developing and debugging complex computer systems, how likely do you believe it is that currently possible efforts could produce error-free software, or even software whose reliability is acceptable given the risks in (1) ?

Clearly answering (3) requires subjective judgements, but computer professionals are among the best people to ask to make such judgements given their expertise.

I think it would be rather amusing if you told the press what you told bboard: that you "hope they can get it to work".

Software engineering and SDI

Date: 16 Aug 85 2200 PDT

To: su-bboards@SU-AI.ARPA From: John McCarthy <JMC@SU-AI.ARPA> Subject: sdi

I thank those who advised me on whether to say something about the SDI controversy in my lecture or at the press conference. I don't presently intend to say anything about it in my lecture. Mainly this is because thinking about what to say about a public issue would interfere with thinking about AI. I may say something or distribute a statement at the press conference.

I am not sure I understand the views of those who claim the computer part of SDI is infeasible. Namely, do they hope it won't work? If so, why? My reactionary mind thinks up hypotheses like the following. It's really just partisanship. They have been against U.S. policy in many areas including defense, that they automatically oppose any initiative and then look for arguments.

Software engineering and SDI

Date: Thu, 15 Aug 85 13:01:46 pdt From: vax-populi!dparnas@nrl-css (Dave Parnas) To: Neumann@SRI-CSLA.ARPA Subject: Re: [John McCarthy <JMC@SU-AI.ARPA>: IJCAI as a forum]

McCarthy is making a classic error of criticizing something that he has not read. I have not argued that any program cannot be written and debugged. I argue a much weaker and safer position, that we cannot know that the program has been debugged. There are "fundamental computer science reasons" for that, they have to do with the size of the smallest representation of the mathematical functions that describe the behaviour of computer software and our inability to know that the specifications are correct.

Dave

Date: Thu, 15 Aug 85 13:14:22 pdt From: vax-populi!dparnas@nrl-css (Dave Parnas) To: neumann@SRI-CSL.ARPA Subject: Copy of cover letter to Prof. John McCarthy

Dear Dr. M

A friend of mine, whose principal weakness is reading the junk mail posting on bulletin boards sent me a copy of your posting with regard to SDI.

It is in general a foolish error to criticize a paper that you have not read on the basis of press reports of it.

Nobody has, in fact, claimed that any given program cannot be written and "debugged" (whatever that means). The claim is much weaker, that we cannot know with confidence that the program does meet its specification and that the specification is the right one. There is both theoretical (in the form of arguments about the minimal representation of non-continuous functions) and empirical evidence to support that claim. The fact that you do not read the literature on software engineering does not give you the authority to say that there are no papers supporting such a claim.

As I would hate to see anyone, whether he be computer scientist or AI specialist, argue on the basis of ignorance, I am enclosing ...

Software engineering and SDI

Date: Thu 15 Aug 85 18:50:46-PDT From: Gary Martins <GARY@SRI-CSLA.ARPA> Subject: Speaking Out On SDI To: jmc@SU-AI.ARPA

Dear Dr. McC -

In response to your BB announcement:

1. Given that IJCAI is by and large a forum for hucksters and crackpots of various types, it is probably a poor choice of venue for the delivery of thoughts which you'd like taken seriously by serious folks.

2. Ditto, for tying your pro-SDI arguments in with "AI"; it can only lower the general credibility of what you have to say.

3. You are certainly right that no-one can now prove that the creation of effective SDI software is mathematically impossible, and that part of your argument is beyond reproach, even if rather trivial. However, you then slip into the use of the word "impractical", which is a very different thing, with entirely different epistemological status. On this point, you may well be entirely wrong -- it is an empirical matter, of course.

I take no personal stand on the desirability or otherwise of SDI, but as a citizen I have a vested interest in seeing some discussions of the subject that are not too heavily tainted by personal bias and special pleading.

Gary R. Martins Intelligent Software Inc.

International Conference on Software Engineering 28-30 August 1985, London UK Feasibility of Software for Strategic Defense Panel Discussion 30 August 1985, 1:30 - 3:00 PM

Panelists:
Frederick P. Brooks III, University of North Carolina David Parnas, University of Victoria Moderator: Manny Lehman, Imperial College

This panel will discuss the feasibility of building the software for the Strategic Defense System ('Star Wars') so that that software could be adequately trusted to satisfy all of the critical performance goals. The panel will focus strictly on the software engineering problems in building strategic defense systems, considering such issues as the reliability of the software and the manageability of the development.

[This should be a very exciting discussion. Fred has extensive hardware, software, and management experience from his IBM OS years. David's 8 position papers have been widely discussed -- and will appear in the September American Scientist. We hope to be able to report on this panel later (or read about it in ARMS-D???). Perhaps some of you will be there and contribute your impressions. PGN]

Date: Mon, 15 Jul 85 11:05 EDT From: Tom Parmenter

From an article in Technology Review by Herbert Lin on the difficulty (impossibility) of developing software for the Star Wars (Strategic Defense Initiative) system:

Are there alternatives to conventional software development? Some defense planners think so. Major Simon Worden of the SDI office has said that

"A human programmer can't do this. We're going to be developing new artificial intelligence systems to write the software. Of course, you have to debug any program. That would have to be AI too."

Date: Wed, 14 Aug 85 18:08:57 cdt From: uwmacc!myers@wisc-rsch.arpa (Latitudinarian Lobster) Message-Id: <8508142308.AA12046@maccunix.UUCP> To: risks@sri-csl.arpa Subject: CPSR-Madison paper for an issue of risks?

The following may be reproduced in any form, as long as the text and credits remain unmodified. It is a paper especially suited to those who don't already know a lot about computing. Please mail comments or corrections to:

Jeff Myers [Something was lost here...] University of Wisconsin-Madison reflect the views of any other Madison Academic Computing Center person or group at UW-Madison. 1210 West Dayton Street Madison, WI 53706 ARPA: uwmacc!myers@wisc-rsch.ARPA UUCP: ..!{harvard,ucbvax,allegra,heurikon,ihnp4,seismo}!uwvax!uwmacc!myers BitNet: MYERS at MACCWISC

COMPUTER UNRELIABILITY AND NUCLEAR WAR

Larry Travis, Ph.D., Professor of Computer Sciences, UW-Madison Daniel Stock, M.S., Computer Sciences, UW-Madison Michael Scott, Ph.D., Computer Sciences, UW-Madison Jeffrey D. Myers, M.S., Computer Sciences, UW-Madison James Greuel, M.S., Computer Sciences, UW-Madison James Goodman, Ph.D., Assistant Professor of Computer Sciences, UW-Madison Robin Cooper, Ph.D., Associate Professor of Linguistics, UW-Madison Greg Brewster, M.S., Computer Sciences, UW-Madison

Madison Chapter Computer Professionals for Social Responsibility June 1984

Originally prepared for a workshop at a symposium on the Medical Consequences of Nuclear War Madison, WI, 15 October 1983

[The paper is much too long to include in this forum, but can be obtained from Jeff Myers at the above net addresses, or FTPed from RISKS@SRI-CSL:<RISKS>MADISON.PAPER. The section headings are as follows:

- 1. Computer Use in the Military Today, James Greuel, Greg Brewster
- 2. Causes of Unreliability, Daniel Stock, Michael Scott
- 3. Artificial Intelligence and the Military, Robin Cooper
- 4. Implications, Larry Travis, James Goodman
-]

Date: Wed, 21 Aug 85 17:46:55 PDT From: Clifford Johnson <GA.CJJ@Forsythe> To: SU-BBOARDS@SCORE Subject: @= Can a computer declare war?

*********************** CAN A COMPUTER DECLARE WAR?

Below is the transcript of a court hearing in which it is was argued by the Plaintiff that nuclear launch on warning capability (LOWC, pronounced lou-see) unconstitutionally delegates Congress's mandated power to declare war.

The Plaintiff is a Londoner and computer professional motivated to act by the deployment of Cruise missiles in his hometown. With the advice and endorsement of Computer Professionals for Social Responsibility, on February 29, 1984, he filed a complaint in propria persona against Secretary of Defense Caspar Weinberger seeking a declaration that peacetime LOWC is unconstitutional. The first count is presented in full below; a second count alleges a violation of Article 2, Part 3 of the United Nations Charter which binds the United States to settle peacetime disputes "in such a manner that international peace and security, and justice, are not endangered":

1. JURISDICTION: The first count arises under the Constitution of the United States at Article I, Section 8, Clause 11, which provides that "The Congress shall have Power ... To declare War"; and at Article II, Section 2, Clause 1, which provides that "The President shall be Commander in Chief" of the Armed Forces.

2. Herein, "launch-on-warning-capability" is defined to be any set of procedures whereby the retaliatory launching of non-recoverable nuclear missiles may occur both in response to an electronically generated warning of attacking missiles and prior to the conclusively confirmed commencement of actual hostilities with any State presumed responsible for said attack.

3. The peacetime implementation of launch-on-warning-capability is now presumed constitutional, and its execution by Defendant and Defendant's appointed successors is openly threatened and certainly possible.

4. Launch-on-warning-capability is now subject to a response time so short as to preclude the intercession of competent judgment by the President or by his agents.

5. The essentially autonomous character of launch-on-warning-capability gives rise to a substantial probability of accidental nuclear war due to computer-related error.

6. Said probability substantially surrenders both the power of Congress to declare war and the ability of the President to command the Armed Forces, and launch-on-warning-capability is therefore doubly repugnant to the Constitution.

7. The life and property of Plaintiff are gravely jeopardized by the threat of implementation of launch-on-warning-capability.

WHEREFORE, Plaintiff prays this court declare peacetime launch-on-warning-capability unconstitutional.

***************** THE HEARING IN THE COURT OF APPEALS FOLLOWS

[in the original message, and is too lengthy to include here. I presume you will find it in ARMS-D -- see my interpolation into the note from Bob Carter above. Otherwise, you can FTP it from SRI-CSL:<RISKS>JOHNSON.HEARING. PGN]



Search RISKS using swish-e

Report problems with the web pages to the maintainer



Dave Curry <davy@purdue-ecn.ARPA> Thu, 29 Aug 85 21:22:44 EST

Just some miscellaneous comments on some of the things in RISKS V1#2. Hope this isn't too long.

- Fishermen. This sounds like a crock to me. I wonder whether the broken buoy or the fact that the storm was not predicted was the deciding factor in the case. Since the NWS/NOAA is providing a service, which nobody is *required* to use, I can't understand how they can be sued for not predicting a storm. What would happen if they predicted a storm which never showed up? Could all the fishermen who stayed home sue for their lost profits? I can see it now.... "Cloudy Thursday, rain Friday -- use this information at your own risk."
- 2. Union Carbide. I always wonder in cases like this whether the plant is actually having more accidents than usual, or if because of Bhopal we're just hearing about it more because the press has a new victim to pick on. The number of accidents at that plant is disgraceful. Does anyone think the government will shut it down?
- 3. Bob Carter's comments. I think I agree with PGN on these... I would prefer to see RISKS cover more or less anything related to computer "hazards", rather than centering on one or two things. There are plenty of other lists which already take certain parts of this (e.g. SOFT-ENG for "who's responsible" type stuff, ARMS-D for SDI). I also like the SEN quotes -- I don't personally read SEN, and even if some of the stuff is dumb (computer kills scientist), overall I think the brief summary PGN provided in V1 #1 gives a nice broad range of topics to discuss.
- 4. Medical programs. I'm not sure I trust these fully yet. I'd have no qualms about my doctor using one to *suggest* things to him, but I would draw the line at his accepting the program's diagnosis unless he could verify on his own that it was correct. For example, a heart specialist interpreting a heart-diagnosis program's output would be good; a general practicioner's taking it as gospel would not be good. We need to make sure the doctor is capable of knowing when the program is wrong. (I saw a comment about MYCIN once "if you brought MYCIN a bicycle with a flat tire, it would try like hell to find you an antibiotic.")

 SDI. I'm going to leave this for the experts. I personally lean towards Parnas's "side", but I don't know enough about it. I do like reading the comments on it though. (BTW, for those of you who haven't yet read Herb Lin's paper, it's excellent.)

Great list so far... keep it coming. As a (possibly) new topic, did anyone go to this AI show in San Diego (?) or wherever? I saw a blurb on it somewhere... how about a review of what the current toys are and what risks they may take? I remember seeing something about a program to interpret the dials and gauges of a nuclear power plant....

--Dave Curry davy@purdue-ecn

Computer/hardship list

Rosenberg Jerome <jerome@wisc-rsch.arpa> Thu, 29 Aug 85 14:00:58 cdt

Peter: One basis for a focussed discussion of risks would be to try to establish a list of those computer systems whose failure would cause great hardship --economic, political, social --to a significant number of our citizens. For example, the failure of our computer-controlled electric power grid or the failure of the Reserve's check clearance system.

Your readers/participants could be asked to suggest the systems to be included on the list. Your forum could then discuss probabilies of failure, costs of failures vs failure time, etc. etc..

Jerry

Medical KBES

Ave decus virginum! <goun%cadlac.DEC@decwrl.ARPA> Friday, 30 Aug 1985 05:37:48-PDT

Some AI systems may need FDA approval

Expert systems come within the FDA ambit to the extent that they supplement doctor's work, according to Richard Beutal, a Washington D.C. attorney specializing in the legal aspects of technology.

An expert system may be defined as a computer program that embodies the expertise of one or more human experts in some domain and applies this knowledge to provide inferences and guidance to a user. some of the earliest and most sophisticated systems were developed for medical diagnosis: MCYIN, EMCYIN, CADUCEUS AND ATTENDING. [There are several more in use in Japan. --mjt]

Beutal called attention to proposed FDA regulations that, if implemented, would require medical expert systems to obtain FDA pre-marketing approval. Given that FDA approval for what are class 3 devices could take up to 10 years and that reclassifying such devices can take almost as long, these FDA regulations would virtually cause investment to dry up.

{Government Computer News Aug 16, 1985}

Mealth hazards of CRT use

Robin Cooper <cooper@wisc-ai.arpa> Thu, 29 Aug 85 10:35:20 cdt

With respect to the introduction of the topic of the health hazards of using video terminals, I would be particularly interested in seeing discussion of risks to pregnant women and their unborn children. Both Sweden and Canada have apparently introduced legislation which gives pregnant women the right to change job assignments, whereas the official US line seems to be that there is not sufficient risk to warrant this.

Robin Cooper



Search RISKS using swish-e

Report problems with the web pages to the maintainer



Peter G. Neumann <<u>Neumann@SRI-CSLA.ARPA</u>> Mon 2 Sep 85 14:05:15-PDT

The issue of the lobstermen indeed rested on the negligence of not repairing the buoy. (As noted in RISKS-1.2, the weather buoy went unrepaired for three months.)

Negligence and inaction in the presence of informed knowledge are likely to be the source of more lawsuits in the future. For example, the NY Times of 1 September 85 had an article by Richard Witkin on KAL 007.

Evidence introduced in lawsuits filed in connection with the Soviet downing of the Korean Air Lines Flight 007 suggests that American radar operators knew hours beforehand that the jetliner was off course and heading into Soviet airspace.

The words, "We should warn him", presumably referring to the plane's pilot, were heard at the Government's civil air-traffic control station in Alaska as the Boeing 747 strayed off course toward its fatal encounter with a

Soviet fighter plane two years ago today, according to the documents.

The documents were submitted Friday as evidence in damage suits filed against the United States Government by relatives of the 269 people who died in the incident.

Medical malpractice suits have been on the upswing, and doctors are taking extraordinary measures to compensate -- such as higher prices and otherwise unnecessary tests and drugs. But the question of what constitutes computer-related malpractice is likely to emerge as a very sticky one, e.g., faulty computer system design, life-critical application programming, and sloppy computer operation. And what about a debugger or maintainer who notices something fishy but does not carry through? A remarkable case of a casual observer playing a significant role took place on 1 Sept 85 when a passenger on People Express Flight 183 from Dulles to Newark noticed minutes after take-off that a cowling was missing on one of the engines. (The plane returned to Dulles.) Imagine a lawsuit against a company, which in turn sues the programmer. The potential for legal confusion relating to computer systems is really quite awesome, and the confusion has just begun. Suppose the windshear-warning system is finally installed (with the 31 May 84 near-disaster on take-off of a UA 727 and the recent crash providing an impetus), and suppose that program has a bug? Suppose the computer is not working on landing? There are some very serious questions that must be raised. The incidence of high-award law suits elsewhere is likely to provide a strong forcing function.

Re: health hazards of CRT use

Brint Cooper <<u>abc@BRL.ARPA</u>> Fri, 30 Aug 85 21:56:09 EDT

To balance this discussion, we need to include risks to pregnant women and their born and unborn children of television sets that run 18 hours a day in the home.

Keep in mind: X-radiation is generally produced by the very high voltages traditionally used in color television sets and composite-video color monitors. Many of the monochrome monitors need no such voltages and, so, produce no such radiation.

Since most folks are now buying color TVs for their homes, we need to examine that aspect of safety as well, especially since many of them are used as monitors for home computers and video games.

Brint Cooper

Re: health hazards of CRT use

Robin Cooper <<u>cooper@wisc-ai.arpa</u> > Sun, 1 Sep 85 12:13:49 cdt Yes, that seems right, though I wonder what the facts are concerning how close one sits to the device. People spend more time a few feet away from their terminals than their TVs.

Robin Cooper

Re: health hazards of CRT use

Peter G. Neumann <<u>Neumann@SRI-CSLA.ARPA</u>> Mon 2 Sep 85 21:10:33-PDT

To: RISKS@SRI-CSLA.ARPA

There is also discussion in the literature on physical and psychological problems resulting from sitting in front of your terminal for hours, most notably back and neck problems, tension, stress, anxiety, and subsequent depression. This forum is not really the place to discuss another relevant aspect of the problem, but let me just mention it anyway and then discourage further commentary on it: the standard American junk-food diet of coffee, colas, and caffeine generally, orange juice, sugar, chocolate (containing both sugar and caffeine), refined white flour, fried foods, and so on, is now being linked with making many of those problems worse.

×

Brint Cooper <<u>abc@BRL.ARPA</u>> Fri, 30 Aug 85 22:00:55 EDT

cc: risks@SRI-CSL.ARPA Subject: Medical Software

Actually, culpability for mistakes caused by medical diagnosis software could be placed with the same person who is responsible for correct interpretation of all diagnosis aids: the physician him/herself. Programmers, like authors of medical texts, are providing tools for the physician, not replacing him or her.

What we CAN do as computer scientists, et al., is to educate the medical profession to the limitations of these tools as well as to their benefits. For ourselves, the goals should include error and risk reduction as we continue to discuss.

Brint

Kolm's Hawk-32

Doug Bryan <<u>BRYAN@SU-SIERRA.ARPA</u>> Sat 31 Aug 85 22:58:00-PDT

Speaking of possible hazards due to hardware failure, has anyone out there

had any experience with Rolm's 32 bit Mil Spec machine the Hawk-32? Since the Hawk is a Mil Spec machine, I'm sure it will be used in situations where failure could lead loss of life.

I would be interested in hearing about the Hawk's environment limitations, mean time between failures and any other experiences people have had with the machine.

doug

[POSTSCRIPT: A few of you complained that the first issue had too much of a military flavor. It is interesting that except for this last item, this issue and the previous issue had almost none! On the other hand, the problems we are dealing with are universal, and we should be able to learn from all relevant discussions...

I had some complaints about the format breaking your dedigestifying programs. I hope this is better, but if it really is, your programs must be pretty stupid. I did not change anything except the trailer. So maybe I don't have it right yet?

Others complained that the issues were too big and did not come out often enough. (I explained why -- I wasn't around.) Now you will undoubtably complain that that they are too small and too frequent. But it really depends on what contributions are available. 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

Search RISKS using swish-e

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

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

Feeds

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

Smartphone (latest issue) Under Development!!

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

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

Selectors for locating a particular issue from a volume

Volume number: Issue Number:

Volume Index

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

Index to the RISKS Digest

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

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



<u>SCRIBE time-bomb goes off! (Peter G. Neumann)</u>

Issue 6 (4 Feb 86)

- Shuttle computers (Marc Vilain) -- from NY Times
- SRBs and Challenger (Mike Iglesias) -- from LA Times
- Galileo, Plutonium, Centaur, physical security [4 messages] (Henry Spencer)
- RISKS-2.5 & "Some simple calculations" (Bob Ayers)
- <u>A hard rain is gonna fall. (Herb Lin)</u>
- By the slip of a finger ... (Ted Lee)

Issue 7 (6 Feb 86)

- The lesson of Challenger (Barry Shein)
- Mistaken Arrest due to computer error (Steve Rabin)
- Denial of [Religious] Service (Chris Guthrie)
- Earthquake Monitoring Systems (Gary T. Leavens)
- Mice & CRT Radiation (Ted Shapin)
- SRBs, What the Computers Should Monitor, and Expert Systems? (Jim Giles)
- Redundancy in the Shuttle's Computers (K. Richard Magill)
- Nuclear Cargo in the Shuttle (Larry Shilkoff)
- Software Protection Symposium (Barbara Zayas)

Issue 8 (7 Feb 86)

- Expert systems and shuttles (Michael Brown, Dave Platt)
- Plutonium (Martin J. Moore)
- Earthquake Monitoring Systems (Mike Raugh via Matt Bishop, Hal Murray, Eugene Miya)
- Issue 9 (9 Feb 86)
 - Computerized train wreck? ... Computer-induced stock-market swings. (Martin Minow)
 - Selectively Displaying Data -- Boeing 767 EFIS (Alan M. Marcum)
 - Cape Range Safety Display Systems (Lynne C Moore)
- Issue 10 (12 Feb 86)
 - Computerized aircraft collision avoidance (Peter G. Neumann)
 - Computerized Feedback and the Stock Market (Eric Nickell)
 - <u>Analyst Changes City Treasurer's Computer Code (Mike McLaughlin)</u>
 - Plutonium on the Space Shuttle (Tom Slone)
 - Request to RISKS Readers from COMPASS 86 (COMPuter ASSurance) (AI Friend)
- Issue 11 (16 Feb 86)
 - SF Federal Reserve Bank 2 Billion Dollar Goof (SF Chron via Peter G. Neumann)
 - Washington D.C. Analyst's Password Game (AP via Geoff Goodfellow)
 - Boeing 767 EFIS -- compare Airbus A320 (Rob Warnock)
 - <u>Networks Pose New Threats to Data Security (InfoWorld-86/2/10 via Werner Uhrig)</u>
- Issue 12 (18 Feb 86)
 - Risks in automobile microprocessors -- Mercedes 500SE (Peter G. Neumann)
 - Train safeguards defeated (Chuck Weinstock)
 - Security Safeguards for Air Force Computer Systems (Dave Platt)
 - How can Alvin Frost fight City Hall? (Jim DeLaHunt)
 - More Plutonium/Shuttle (Martin J. Moore)
 - Computerized Voting -- talk by Eva Waskell (Wednesday eve, 19 February, MIT)

Issue 13 (20 Feb 86)

- Dec. 8 cruise missile failure caused by procedural problems (Martin J. Moore)
- <u>Computerized voting (Matt Bishop)</u>
- Non-science quotations on Plutonium (Bob Ayers)
- Software Piracy (D.Reuben)
- <u>Air Force Security Safeguards (Stephen Wolff)</u>
- Shuttle Safety (NYTimes News Summary)

Issue 14 (24 Feb 86)

- Automotive Problems Intensify (Peter G. Neumann)
- A hard rain is gonna fall (around March 23) (Martin J. Moore)
- Misdirected modems (Alan Silverstein)
- Witch hunts, or Where does the buck stop? (M.L. Brown)
- Spells and Spirits (Steve Berlin)
- Issue 15 (25 Feb 86)
 - Software Safety Survey (Nancy Leveson)
 - Titanic Effect (Nancy Leveson)
 - F-18 spin accident (Henry Spencer)
 - Space shuttle problems (Brad Davis)
 - <u>Misdirected modems (Matt Bishop)</u>
- Issue 16 (25 Feb 86)
 - Volunteers to study security of computerized voting booths? (Kurt Hyde)
 - Our Economy Is Based On Electricity (Jared M. Spool)
 - <u>Misdirected modems (Jared M. Spool)</u>
 - The Titanic Effect (Earl Boebert)

Issue 17 (28 Feb 86)

- <u>Replacing humans with computers? (Nancy Leveson)</u>
- Eastern Airlines stock (Steve Strassmann)
- Computerized stock trading and feedback systems (Kremen)
- <u>Computer Voting Booths (Larry Polnicky)</u>
- <u>Reliance on security (Jong)</u>
- Al risks (Nicholas Spies)
- Data Encryption Standard (Dave Platt)

Issue 18 (28 Feb 86)

- Titanic and What did I overlook? (Hal Murray)
- <u>Titanic Effect (Jong)</u>
- Computers placing telephone calls (Art Evans)
- Misdirected modems (Sam Kendall)
- Modems and phone numbers (David Barto)
- Misdirecting my modem (Mike McLaughlin)
- Power-outages, & other failures of central DP systems (Dave Platt)
- <u>Computer voting booths (Dave Platt)</u>
- Data Encryption Standard (Chris McDonald)
- Issue 19 (2 Mar 86)
 - <u>A word from Isaac Asimov about Robots (Bryan)</u>

- <u>Al risks (John Shore)</u>
- Replacing Humans with Computers (David desJardins)
- On-line Slot Machines (Jeff Makey)
- Issue 20 (2 Mar 86)
 - Risks in Encryption (Jerry Saltzer)
 - NSA and encryption algorithms (Curtis Jackson)
 - Low-Tech Computerized Voting (Harry S. Delugach)
 - <u>Risks in ballot-counting systems (Larry Campbell)</u>
 - <u>Misdirected modems (Richard H. Lathrop)</u>
- Issue 21 (3 Mar 86)
 - The risks of (not) using Robots (Hal Murray)
 - <u>Computerized Voting Booths (Larry Polnicky)</u>
 - No-carrier detection by misdirected modems (Dave Platt)
- Issue 22 (5 Mar 86)
 - Voting receipt (Mike McLaughlin)
 - Voting booths (Jim McGrath)
 - Computerized Voting (Tom Benson)
 - Replacing humans with computers (Alan M. Marcum)
 - Electricity's power (Marianne Mueller)
- Issue 23 (6 Mar 86)
 - Computerized voting (Jeff Mogul, Larry Polnicky, Peter G. Neumann)
 - ATM Ripoff (Dave Curry)
 - Internet importance/robustness (Tom Perrine)
- Issue 24 (8 Mar 86)
 - Computerized ballot stuffing (Andy Kegel)
 - Progress report on computerized voting (Kurt Hyde)
 - Wild Modems (Bjorn Benson)
 - Misdirected modems (Phil Ngai)
 - Power outages (Phil Ngai)
 - Earthquake problems with Nuclear Reactors (Lindsay F. Marshall)

Issue 25 (10 Mar 86)

- Balloting (Barbara E. Rice)
- Canceling ballots (Jim McGrath)
- Bank robbery (Curtis Jackson)
- Earthquake problems with Nuclear Reactors (throopw)
- Modems DON'T WORK AS SUPPOSED (Brent Chapman, Martin J. Moore, Phil Ngai)
- Issue 26 (14 Mar 86)
 - Integrity of the Electoral Process (Mark Jackson)
 - Ballot Secrecy (Lindsay F. Marshall)
 - <u>Nuclear waste-land (Jerry Mungle)</u>
 - <u>Nuclear disasters (Lindsay F. Marshall)</u>
 - <u>103/212 modems (Ephraim)</u>
- Issue 27 (15 Mar 86)

- 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)
- <u>Mailer Gone Mad? (Landrum)</u>
- 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)
 - <u>A Stitch in Time (Jagan Jagannathan)</u>
 - <u>Clockenspiel (Jim Horning)</u>
 - <u>Cordless phones (Chris Koenigsberg)</u>
 - 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)
 - <u>Commission vs omission (Geoffrey A. Landis)</u>
 - <u>Stupid Clock Software (Dave Curry)</u>
 - Control characters in headers from eglin-vax (Martin J. Moore)
 - Money Talks (Prasanna G. Mulgaonkar)
- Issue 31 (19 Mar 86)
 - <u>Still more on shuttle destruct systems (Martin J. Moore)</u>
 - <u>Clock Synchronization (Andy Mondore)</u>
 - 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)
 - <u>RSO's and IIP's (Dave Curry)</u>
 - <u>Complex systems ru(i|n)ning our cities (Mike Mc Namara)</u>
 - <u>Re: Two more mailer problems (Bernard S. Greenberg)</u>
 - Banknotes for the visually handicapped (Nigel Roberts, Barbara E. Rice)
 - Psychological and sociological consequences (Harald Baerenreiter)
- Issue 33 (23 Mar 86)

- RSO's and IIP's Martin Moore's response (Dave Curry)
- Omissions/commissions and missile destructs (Chris McDonald)
- Blind and Paper Money (sdo)
- <u>Two Cases of Computer Burglary (NY Times)</u>
- Issue 34 (27 Mar 86)
 - RSO's and IIP's Martin Moore's response (Henry Spencer)
 - Range Safety: a final word (Martin Moore)
 - Someone really sophisticated, with a Ph.D... (Nigel Roberts, Keith F. Lynch)
- Issue 35 (30 Mar 86)
 - San Jose Library (Matthew P. Wiener, Ken Laws)
 - Inter-system crashes (Rich A. Hammond)
- Issue 36 (1 Apr 86)
 - Errant Clocks (Barry Shein)
 - Computer Illiteracy (Matthew P. Wiener)
 - San Jose Library (Dick Karpinski, Holleran)
 - <u>Psychological and sociological consequences (Dave Benson)</u>
 - More inter-system crashes (Henry Spencer)
 - <u>COMPASS 86: A Progress Report (Al Friend)</u>
- Issue 37 (6 Apr 86)
 - Request for information about military battle software (Dave Benson)
 - <u>Programming productivity (Henry Spencer)</u>
 - Space Shuttle Software (via PGN)
 - Open-and-Shut Case Against Reagan's Command Plane (Geoffrey S. Goodfellow)
 - Computer Illiteracy (Matt Bishop)
- Issue 38 (8 Apr 86)
 - The UK Driving Vehicle Licensing Centre (Brian Randell)
 - Computer crime wave (Chris Hibbert)
 - Programming productivity (Herb Lin)
 - Request for information about military battle software (Scott E. Preece)
 - <u>Aviation Week Technical Survey: AI & Aviation (Werner Uhrig)</u>
- Issue 39 (11 Apr 86)
 - \$36 million accounting mistake (Graeme Hirst)
 - <u>Admissability of computer files as evidence? (Kathryn Smith)</u>
 - "Rapid advance" of SDI software (Walt Thode)
 - Blame-the-computer syndrome (JAN Lee)
 - Hackensack Phone Snafu (Dirk Grunwald)
- Issue 40 (12 Apr 86)
 - GREAT BREAKTHROUGHS [Red Herrings swimming upstream?] (Dave Parnas)
 - Military battle software ["first use", "works"] (James M Galvin, Herb Lin, Scott E. Preece, Dave Benson)
 - First use Enterprise (Lindsay F. Marshall)
- Issue 41 (13 Apr 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)
- <u>Review of *Softwar* (Gary Chapman)</u>
- 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)
- <u>Star Wars software advance (AP)</u>
- Smart bombs in Libya (Washington Post)
- Pacific Bell Bills (SF Chronicle)
- <u>BU joins the InterNet... (Barry Shein)</u>

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)
- <u>SDI (Larry Campbell)</u>
- 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)
- <u>Strategic Systems Reliability Testing (Herb Lin)</u>
- <u>Correction on Challenge Discussion (Jeff Siegal)</u>

Issue 48 (3 May 86)

- Failure to Backup Data (James H. Coombs)
- Computer detracting from effective communication? (Bruce A. Sesnovich)
- Words, words, words... (Mike McLaughlin)
- Copyright Laws (Matthew Kruk)
- Re: Correction on Challenger (Martin J. Moore)

Issue 49 (7 May 86)

- Perrow on reactor containment vessels (Richard Guy)
- Captain Midnight (Scott Dorsey, MRB)
- NSA planning new data encryption scheme they'll keep the keys (Jon Jacky)
- Espionage (Mike McLaughlin)
- The Star Wars Swindle (Dave Weiss)
- Backups (Will Martin)
- Interpreting Satellite Pictures (Lindsay F. Marshall)
- Word-processing damages expression (Niall Mansfield, PGN)
- Proofreading vs. computer-based spelling checks (Dave Platt)
- Issue 50 (8 May 86)
 - Refocus the discussion, please! (Bob Estell)
 - [Response.] Also, Delta rocket shutdown (Peter G. Neumann)
 - Large systems failures & Computer assisted writing (Ady Wiernik)
 - DESisting (dm, William Brown II)
 - Failure to Backup Data (Greg Brewster)
- Issue 51 (11 May 86)
 - Reliability limits (Brian Randell)
 - NSA assigning encryption keys (Jay Elinsky)
 - HBO pirate (Lauren Weinstein)
 - Failure to Backup Data, by James H. Coombs (Roy Smith)
 - <u>Admissibility of legal evidence from computers (Mike McLaughlin)</u>
 - Electronic document media (Mike McLaughlin)
- Issue 52 (13 May 86)
 - Launch failures (Phil R. Karn)
 - <u>Brittleness of large systems (Dave Benson)</u>
 - HBO (Scott Dorsey, Dave Sherman)
 - Word processing -- reroute [reroot?] the discussion (Chuq Von Rospach)
- Issue 53 (16 May 86)
 - A late report on the Sheffield (AP [from Martin Minow], LA Times [Dave Platt]
 - <u>News items [Lobsters; Eavesdropping] (Alan Wexelblat)</u>
 - More Phone Bill Bugs... (Dave Curry)
 - Backup problems (Davidsen, Roy Smith)
- Issue 54 (25 May 86)
 - Meteorites (Larry West)
 - Meteorites, Chernobyl, Technology, and RISKS (Peter G. Neumann)
 - London Stock Exchange Computer System Crash (Lindsay F. Marshall)
 - Backup (Fred Hapgood, Bruce O'Neel)

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)

4 🕤 🕨 🥖 📝

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....



*****The Strategic Defense Initiative

Joseph Weizenbaum <JOSEPH@MIT-XX.ARPA> Wed 4 Sep 85 14:19:15-EDT

Greetings !

I've just been introduced to the RISKS b-board you have undertaken to maintain. It is a good idea. What stimulates this particular outburst is John McCarthy's observation that many of the computer people who maintain that Star Wars can't be made to work for technical reasons, e.g., those brought forth by Parnas, are people who have opposed many other government initiatives. I imagine he means among others the war on Viet Nam, the MX missile, the ABM initiative of years ago, the administration's policies vis-a-vis Nicaragua, Cuba and El Salvador, and so on and on.

I confess I've been on what from John's point of view must be characterized as the wrong side on each of the above controversies. But then John has been on what I would have to see as the wrong side on all these questions. Does that relieve me of the obligation to guard my intellectual honesty by studying his actual arguments ? If so, then the very possibility of dialog between holders of opposing views becomes impossible.

It is, however, important for people who indeed have a point of view to make their positions clear, at least not to hide them. Their doing so ought not to disqualify what they then have to say. For myself, I find it even more important to actually draw on my quasi pacifist position in arguing about Star Wars and similar issues and to explicate the connections I make. I do believe (with Parnas and many others) that the software required simply cannot be produced to the degree of confidence without which it would be a meaningless exercise. I don't want to rehash the various technical arguments here, however. Let me just rest on the well publicized statements of CPSR and of Parnas. I want to say in addition, however, that I would not support the SDI initiative even if I thought it to be technically feasible. In that, John is guite right. I'm afraid that many of the computer people who rest on the technical arguments alone leave the impression that these alone constitute their objections to the program. Perhaps that is the position of many objectors in the computer community. I think, however, there are many who would join me in resisting the program even if it could be shown to be technically feasible. I think John is quite right in asking that that be made explicit where it applies.

This is not the place to air political and ideological positions. For clarity's sake, I just want to add to the above that I believe it to be necessary to the survival of us all that we come to some social, political, cultural accommodation with the rest of the peoples of the world even when, or especially when, they organize their societies differently than we do ours. SDI is in the tradition of the great technological fixes which appear to their authors to relieve them of the responsibility to confront underlying human problems.

Besides, SDI is a giant step to the further militarization of space and of our society. I oppose that as well.

Joseph Weizenbaum.

[For those of you just returning from the London 8th International Conference on Software Engineering, we eagerly await reports on the panel session of Fred Brooks and Dave Parnas on the feasibility of SDI from the software engineering point of view alone.

You will find a lengthy special report on "Star Wars" in the IEEE Spectrum, September 1985. My copy arrived today.

SDI: The Grand Experiment Part 1 -- Mind-boggling complexity Part 2 -- Exotic weaponry Part 3 -- Debating the issues

PGN]

✓1.5 Million Ford Engines Need Recall?

Hal Murray <Murray.pa@Xerox.ARPA> Tue, 3 Sep 85 12:18:36 PDT

This morning, my radio said something about a consumer group wanting Ford to recall 1.5 million engines. Nobody knows what's wrong, but they are blaming it on the computer. (I didn't get the fine print. I wasn't awake.) Anybody know if that's the real problem or just a convenient scapegoat?

[The 4 Sept 85 NY Times has a note on the recall of 454,000 Chevy/Pontiac compacts for corroding pollution control equipment, and 105,000 VW and Audi cars for faulty brake hoses, but nothing on Ford. I would love to follow up on the 1.5 million Fords, but haven't found anything yet. PGN]

Kisks in CAD, etc.

Eugene Miya <eugene@AMES-NAS.ARPA> 3 Sep 1985 0859-PDT (Tuesday)

Something, I have been wondering about, perhaps for future discussion might concern liabilities of CAD products. It seems more merchandise I purchase is shoddy, and I am beginning to wonder what some of the consequences of "making the metal a bit thinner to save.." could be. I realize we are using CAD and simulation tools to make things more efficient, perhaps the case of the over efficient engine which flamed out when it flew through rain [as reposted in SEN, I believe] might be a case in point. What were our margins of safety in the over-engineering we did in the past? Any studies yet?

Lastly, regarding mail formats: I have run on a gamut of different mailers [my current one, mh, is not bad], but I can sympathize with those having problems. It seems Peter's comment about programs was a bit harsh. I used to read netmail on an IBM machine which concatentated all letters and was destructive [read once mail].

--eugene miya NASA Ames Research Center

Mike McLaughlin <mikemcl@nrl-csr> Wed, 4 Sep 85 18:22:22 edt

It is important we separate crt from non-crt risks. X-rays, color-perception, & possibly eye fatigue I see as crt related. Posture may be, for a person tied to the tube for extended periods. Junk food is a non-crt risk, but may be a denial-of-service risk, if introduced into certain apertures around the crt. Might also be a hazard to your health, if conductive.

X- & like radiation: I am done producing children, I hope. So does my wife. Unless radiation reaches carcinogenic levels, I am not concerned for me. My children all use/will use crts, unless some other display becomes more economical in the near future. We have 5 children, all of age. I am concerned about them.

Posture: As an occasional, voluntary, crt user, my posture is my problem. Take the paper out of my office; or give me a clerical/data entry type job; then I will see posture as a crt/computer risk. Any obstetrician will worry about any woman who sits in any one position for long periods. At one point in one pregnancy my wife had to fly home while I drove alone - solely so she would not have to sit still too long. (Many years ago I was told that the blood supply to the brain passed through the peri-anal region. This accounts for the number of dumb comments and sleeping attendees at various conferences with inadequate breaks.)

Color-perception: When I go home after dark tonight, the white line will be pink. No, I'm not on anything. If the screen were pink, the line would be green. If color sensitivity mattered to me... say, if I performed color-matching titrations in a hospital, or put color-coded resistors & capicators into non-ICs, I would worry about color perception.

Considering the liability discussion in V1 #4, perhaps we all should. In 1956 or 1957 I ran across the proceedings of something-or-other on human factors in submarine design. Book was pretty beat up, so it had been around for a while. It cited some *railroad safety* research on color perception. I think the RR stuff was pre WW-II. Said red & green were neat colors for signal lights. Also said *yellow symbols on a black background* were the best combination for a symbolic display... and that the reverse was the next best. Hence, road signs. Amber screens... ?

Eye-fatigue: Not crt-unique, but... look at anything long enough, your eyes will tire. Look at anything slightly fuzzy, & your eyes will tire quickly, as they try to focus on the un-focusable.

Summary: If a tired terminal operator hits a tree on the way home, it might be due to poor color perception, fatigue due to poor posture (read: furniture), eye fatigue due to poor colors, poor contrast, fuzzy images. It might be a financial disaster for the firm that employed said deceased. Some attorney might look closely into the work situation, and computers would get a bad name when we are really talking about bad management of the computer-workplace.

- Mike

Computerworld Aug 19 articles

Charlie Spitzer <Spitzer%pco@CISL-SERVICE-MULTICS.ARPA> Tue, 3 Sep 85 13:07 MST Readers may be interested in 2 articles from Aug 19 Computerworld.

page 6. Union Carbide modeling program given wrong data.

Discusses wrong information about gases input to a program that was supposed to model gas cloud dispersal. Notable quote: "These programs have been sold to safety people as opposed to engineers, because [the systems] provide good [public relations], are attractive visually and can provide a fairly inexpensive way of dealing with a problem you hope you'll never have."

page 12. On-line crime suspect system implicated in false arrest.

Discusses case of a NJ woman arrested, strip searched and jailed on two separate occasions because of inadequate information stored in the NCIC computer.

charlie

More on False Arrests

Peter G. Neumann <Neumann@SRI-CSLA.ARPA> Tue 3 Sep 85 13:56:12-PDT

[For those of you who do NOT read the ACM SIGSOFT Software Engineering Notes, here are three items taken from my RISKS column in the July 1985 issue on the subject of false arrests. For those of you who have already read these items, you have come to the last message in this issue and need read no further.]

In the past quarter year, there were two different stories of people winding up in jail due to computer-related snafus, and an earlier story that serendipitously goes along with them.

1. The AnchoRages Of Sin

An article on page 17 of the 15 April 1985 issue of ComputerWorld entitled

``DMV computer error puts innocent motorist in jail"

provides us with another software glitch with harmful side-effects. (Brad Davis [b-davis@@utah-cs.ARPA] was the first to point this one out to me.)

The article (by Kathleen Burton) details how a mistake in programming the new Alaskan Department of Motor Vehicles computer system resulted in a motorist spending a night in a Fairbanks jail. The computer indicated (erroneously) that C. R. Griffin was driving with a suspended license. The article also said that only by human intervention were 400 additional driver's licenses not erroneously suspended. Apparently the database kept records of all violations in the past @i[five] years, but was supposed

to search only over the last @i[two] years for motorists who should be suspended. A programmer was quoted as saying that ``the cost of correcting the mistake [in the program] was insignificant.''

2. Shirley There Must Be a Way Out

And then, on 25 April 1985, the Associated Press ran a story about congressional hearings on the FBI national crime computer. Two incidents were included. The first involved an airline flight attendant who was falsely arrested and detained because of incorrect information in the FBI's national crime computer. Sheila Jackson Stossier was arrested on 28 October 1983 at the New Orleans airport, because a woman named Shirley Jackson was wanted by Texas authorities. She wound up in jail for the night and detained in Louisiana for five days. She now has an arrest record, and her married name Stossier is listed in the computer as an alias. Coincidentally, another Shirley (Jones) was also wrongly arrested because another woman alias Shirley Jones was listed in the computer -- despite the facts that they had different birthdays, were six inches apart in height, and 70 pounds in weight. ``Despite this, the Sheriff's office refused to drop the charges.'' (To make matters worse, it was later determined that the wanted Shirley was already in jail at the time!)

3. One in Five Warrant Records Were Wrong -- Poor Odds

David Burnham (NY Times News Service) reported the following related story on 12 Feb 1985.

A Michigan man filed suit charging that he was wrongfully arrested five times in 14 months after an arrest warrant for a man using his name was placed in the national computer system of the FBI. The man, Terry Dean Rogan, charged that four of the arrests occurred after Michigan police had made an unsuccessful effort to get the warrant changed. Rogan contends and the police confirm that the man actually being sought was another person using Rogan's stolen identity and credit cards. Rogan, who is 27 years old, is not wanted for any crime.

[The rest of the last story (which goes on for another page) is in the July issue of Software Engineering Notes. It was also BBOARDed earlier, so I did not think it should be recyled again!]



Search RISKS using swish-e

Report problems with the web pages to the maintainer



✓ Joseph Weizenbaum's comments <JOSEPH@MIT-XX.ARPA>: sdi]

Dave Parnas <<u>vax-populi!dparnas@nrl-css</u> > Thu, 5 Sep 85 07:28:56 pdt

Although there is a great deal of truth and wisdom in Weizenbaum's message, I believe that he overlooks the reason that SDI would be destabilizing and another step in the Arms race. It is not because of the stated goals of the program (Reagan's March 1983 speech) but because those goals are not achievable. There would be nothing wrong with rendering ICBMs and other weapons obsolete. On the contrary, everyone should want to see every country, city, and town protected by an impenetrable shield that would free it from the fear of the indiscriminate horror that rained down on Nagasaki and Hiroshima. It is because the SDIO efforts will not lead to technology of that sort, that SDI is the things that Weizenbaum says it is.

I agree with Weizenbaum that we need to seek non-technological solutions. Technology is not likely to provide solutions in a situation where we oppose a power with equally sophisticated technology.

I believe that SDI is one issue where both disarmament and armament supporters could agree. Both sides seek peace through different mechanisms, but neither will find their goals advanced by an untrustworthy "shield".

Dave

✓ Good Risks and Bad Risks

Dave Brandin <<u>BRANDIN@SRI-AI.ARPA</u>> Thu 5 Sep 85 11:40:30-PDT

To: Neumann@SRI-CSL.ARPA

Peter: I love your material that's being generated and produced, but I note that it seems to weigh overwhelmingly against the computer. Aren't people sending you any GOOD stuff? Like with the aid of a computer, 27 lives were saved, etc.? Like using the new NEC fingerprint computer, they were able to match the Stalker's finger-prints in 3 minutes, etc? Maybe you need a Call for Good News?

Dave

Good Risks and Bad Risks

Peter G. Neumann <<u>Neumann@SRI-CSLA.ARPA</u>> Thu 5 Sep 85 23:32:45-PDT

To: RISKS@SRI-CSLA.ARPA Cc: BRANDIN@SRI-AI.ARPA

Today's SF Chronicle had a nice article on "Computer Holds Promise in Diagnosing Heart Disease", in greatly reducing the number of false negatives. But even there are significant risks. Suppose you or your doctor trusts the computer program more because it indeed has fewer false negatives, and now you produce a false negative. We are back to the case of the woman who killed her daughter and tried to kill herself and her son because the computer program had falsely produced an "incurable" diagnosis. (See the July 85 issue of Software Engineering Notes.)

Well, in the first issue of RISKS I recall saying there has got to be more to this forum than just pointing out negative things. I noted hope from the research community, although one of the agonizing things that we have observed in the ACM Special Interest Group on Software Engineering (SIGSOFT) is the enormous gap between the research community and what is actually being done in practice. For critical systems, the ordinary software development techniques are simply not good enough.

Yes, we should of course point out successes. For example, the Shuttle project has had many -- along with its much more visible problems.

Peter

Hot rodding your AT

<<u>Dan_Bower%RPI-MTS.Mailnet@MIT-MULTICS.ARPA</u>> Wed, 4 Sep 85 14:41:38 EDT

In a recent issue of PC Magazine, Peter Norton espoused the idea of substituting a faster clock chip to enhance performance. Now, according to the folk on the Info-IBM PC digest, this may create problems. An off the shelf PC AT is composed of components guaranteed to work to IBM spec, e.g. 6 Mhz. If I increase the clock rate, then the whole rest of the machine has to be up to snuff. If not, a part dies and I pay a nasty repair bill.

Now if I took Mr. Norton's word as gospel, swapped chips and set my PC AT on fire, would he be liable? How about the publisher?

Hazards of VDTs and CRTs

Al Friend, Space and Naval Warfare Systems Command <<u>friend@nrl-csr</u> > Thu, 5 Sep 85 15:23:05 edt

When evaluating the risks associated with various forms of technology it is sometimes useful to have in hand the available data.

The Food and Drug Administration published a study in 1981:

An Evaluation of Radiation Emission from Video Display Terminals

HHS Publication FDA 81-8153

The ionizing, optical, RF and acoustic radiation from a number of terminals was measured. I will briefly quote some of the conclusions of this study.

For ionizing radiation:

3.5 DISCUSSION

Sufficient research information is available to estimate a range of risks of injury from ionizing radiation exposure. Delayed disease, such as heritable mutation or cancer, usually forms a basis for the estimation, expressed in terms of the instances of the effect per person per unit of radiation (rad,rem, or R). The risk estimates form a basis for radiation protection guidelines.

For a VDT operator, the radiation protection guideline for

individuals in the general population is appropriate. The gui





* The risks of not using some technology

John McCarthy <<u>JMC@SU-AI.ARPA</u>> 07 Sep 85 1329 PDT

The problem with a forum on the risks of technology is that while the risks of not using some technology, e.g. computers, are real, it takes imagination to think of them. A further problem with newspaper, magazine and TV discussion of technology is that journalists and free-lance writers tend to run in intellectual mobs. This biases the discussion for everyone, especially when the same journalists read each others writings and call it public opinion. Here are some illustrations.

 Suppose some organization manages to delay interconnecting police data systems on some specious civil liberty grounds.
Suppose some wanted murderer is stopped for a traffic offense but not arrested, because he is wanted in a jurisdiction not connected to the computer system used by the police officer. He later kills several more people. The non-use of computers will not be considered as a cause, and no-one will sue the police for not interconnecting the computers - nor will anyone sue the ACLU. The connection will not even be mentioned in the news stories.

2. No relative of someone killed on U.S. 101 during the 10 years the Sierra Club delayed making it a freeway sued the Sierra Club.

3. No non-smoker who dies of lung cancer in an area newly polluted by wood smoke will sue the makers of "Split wood not atoms" bumper stickers.

Based on past experience, I expect this question to be ignored, but here's one for the risk-of-computers collectors. Is a risk-of-computers organization that successfully sues to delay a use of computers either MORALLY or LEGALLY LIABLE if the delay causes someone's death? Is there any moral or legal requirement that such an organization prove that they have formally investigated whether their lawsuit will result in killing people? As the above examples indicate, the present legal situation and the present publicity situation are entirely unsymmetric.

Here's another issue of the social responsibility of computer professionals that has been ignored every time I have raised it.

The harm caused by tape-to-tape batch processing as opposed to on-line systems.

From the earliest days of commercial computing people have complained about seemingly uncorrectable errors in their bills. The writers don't know enough to connect this with the use of tape-to-tape batch processing. Under such a system when a customer complains, the person who takes the complaint fills out a form. A key puncher punches the form on a card. At the next file-update, this card goes to tape, and a tape-to-tape operation makes the correction. If there is any error in the form or in the key punching, the correction is rejected, and the customer gets the wrong bill again. On-line systems permit the person who takes the complaint to make the correction immediately. Any errors in making the correction show up immediately, and the person can keep trying until he gets it right or ask for help from a supervisor. Not only is the customer better off, but the complaint-taker has a less frustrating job.

My own experience with the difference occurred in 1979 when my wallet was stolen, and I had to tell American Express and Visa. American Express had an on-line system, and the person who took the call was even able to give me a new card number on the spot. The Visa complaint-taker had to look it up on a micro-fiche file and call back, and still they got it wrong. They gave me a new account number without cancelling the old one.

Perhaps this issue is moot now, but I suspect there are still many tape-to-tape systems or systems using modern equipment that still emulate the old systems. Shouldn't computer professionals who pretend to social responsibility take an interest in an area where their knowledge might actually be relevant?

Once upon a time, beginning perhaps in the middle nineteenth century, scientific organizations were active in pressuring government and business to use new technology capable of reducing risk and promoting the general welfare. I have in mind the campaigns for safe water supplies and proper sewage disposal. Here's a new one that involves computer technology.

Theft can be reduced by introducing the notion of registered property. When you buy a television, say, you have the option of buying a registered model, and the fact that it is registered is stamped on it. Whenever someone buys a piece of used registered property he has the obligation of telephoning the registry to check whether the property with that serial number has been reported stolen and recording his ownership. Repairmen are also obliged to telephone either by voice or by keyboard.

Unfortunately, too many computer people imagine their social responsibility to consist solely of imagining risks.

More on SDI (reply to comments on <u>RISKS-1.5</u> statement)

Joseph Weizenbaum <<u>JOSEPH@MIT-XX.ARPA</u>> Sat 7 Sep 85 16:30:11-EDT

To: Neumann@SRI-CSL.ARPA

I've received a number of responses to the remark I made that I would not support the SDI program even if I thought it could be made to work. I have the feeling that, if I try to respond globally, a full blown debate may ensue. That I really don't want to conduct with the bboard as the medium of expression. Nevertheless, I feel obligated to say just a few words in an attempt to clarify some ideas that have probably been misunderstood.

I said that my attitude derives from what I called a "quasi pacifist" position. One writer thought that pacifists are opposed to all forms of self defense. Actually pacifists are often the first to come to the defense of justice being trampled. But the form of their resistance to wrongs is non-violent. It ought also not to be confused with "passive" resistance - Gandhi often pointed out, usually by his own example, that there is nothing passive about non-violent resistance. My use of the term "quasi pacifist" also elicited comment: Am or am I not a pacifist? Let me say I strive to become a pacifist, to grow up to be one. One isn't an adult by
virtue of merely wishing or claiming to be one. Just so with being a pacifist. I am still far from the goal.

People apparently believe that, were the SDI technically feasible there could be no reasonable objections to its development and deployment. Wouldn't it be comforting if every region, every city and village in America had, so to speak, an invisible shield over it which guarded against the invasion of hostile missiles, they ask. Speaking entirely in practical terms, I would remind them that every year tons (perhaps kilotons) of marijuana are smuggled past the U.S. Coastguard and the custom service. Now that technical progress allows the construction of nuclear "devices" smaller than a moderately sized overnight bag, a determined enemy could destroy American cities without "delivering" war heads by air mail at all ! If I were responsible for national security, I would worry if, a few days before the President's traditional State of the Union message, usually delivered to the assembled leadership of all three branches of our government, some foreign embassy evacuated all its personel. Perhaps a nuclear device of moderate size had made its way to Washington and is about to decapitate the government. We can no more bring peace to this globe by putting impenetrable domes over nations than we can halt the violence in our cities by providing everyone with bulletproof clothing. Human problems transcend technical problems and their solutions.

But suppose we could solve the smuggled bomb problem.

I would still oppose SDI.

SDI is an attempt at a technological solution to problems which have their roots in and are social, political, economic, cultural, in other words, human problems. It is an attempt to find solutions under the the light provided by technology when in fact we know them to reside only in the human spirit. That is what guarantees the failure of SDI more surely than its complexity or the impossibility of its being tested.

Beyond all that is the fact that we live in a world of finite resources. The scarcest resource of all is human talent and creativity. The military already commands the time and energy of most American scientists and engineers. Money is another scarce resource on which the military has first call. On the other hand, social services of all kinds are being cut back. Meanwhile the country faces social problems of horrendous dimensions: There is massive, deep poverty in the land. Adequate health care is beyond the reach of millions of citizens and ruinously expensive for many more millions. The schools are spewing out "a rising tide of mediocrity" while a huge fraction of our youth is functionally illiterate. The conditions that brought on the riots in American cities, for example in Watts, have never been attended to - they silently tick away, time bombs waiting to go off.

When resources are limited they must be distributed on the basis of a widely based consensus on priorities. To silently consent to lowering still further the priorities our society assigns to the people's health and education in favor of spending the billions of dollars required above and beyond the already huge military budget for only the first stages of SDI, is, it seems to me, to condone the continuing impoverishment and

militarization of not only America, but of the whole world. Ever more scientists and engineers will be occupied with military work. Ever more industrial workers of many different kinds will be enmeshed in the militarized sectors of society by, for example, being required to have military security clearances. There is a danger that, in the process of the growing militarization of society, a certain threshold, hard to define but terribly real, will be crossed and that, once crossed, there will be no ready road back to a civilian society.

Joseph Weizenbaum

SDI reliability

<<u>mooremj@EGLIN-VAX</u>>

Fri, 06 Sep 85 14:54:52 CDT

[Peter, I have also posted this to SOFT-ENG. If you think the duplication is reasonable, please include it in RISKS as well. -- mjm]

I've been thinking about the SDI system and how it will be implemented. Specifically, I've been looking at a system composed of N independent platforms, each of which performs its own detection, decision making, and response. Given this type of system, we can reach a few conclusions about the reliability of the whole system, based on the reliability of a single platform. I've crunched a few numbers: nothing profound, just some basic statistics.

Definitions:

- A "false positive" is an attack response by a platform when such a response is not justified.
- A "false negative" is failure of a platform to attack when an attack response is justified.

Let's look at the false positive case first. How likely is the system to experience a false positive, based on the probability for each platform?

	N:	5	0 100	200	500	10	00	2000		
Pp:	+								-	
1.000	E-12		5.000E-11	1.000E-10	2.000E	-10	5.000	E-10	1.000E-09	2.000E-09
1.000	E-11		5.000E-10	1.000E-09	2.000E-	-09	5.000	E-09	1.000E-08	2.000E-08
1.000	E-10		5.000E-09	1.000E-08	2.000E	-08	5.000	E-08	1.000E-07	2.000E-07
1.000	E-09		5.000E-08	1.000E-07	2.000E	-07	5.000	E-07	1.000E-06	2.000E-06
1.000	E-08		5.000E-07	1.000E-06	2.000E	-06	5.000	E-06	1.000E-05	2.000E-05
1.000	E-07		5.000E-06	1.000E-05	2.000E	-05	5.000	E-05	1.000E-04	2.000E-04
1.000	E-06		5.000E-05	1.000E-04	2.000E	-04	4.999	E-04	9.995E-04	1.998E-03
1.000	E-05		4.999E-04	9.995E-04	1.998E-	-03	4.988	E-03	9.950E-03	1.980E-02
1.000	E-04		4.988E-03	9.951E-03	1.980E-	-02	4.877	E-02	9.517E-02	1.813E-01
1.000	E-03	Ι	4.879E-02	9.521E-02	1.814E-	-01	3.936	E-01	6.323E-01	8.648E-01

Pp is the probability that a given weapons platform will experience a false positive. N is the number of platforms in the system. The entries in the

table give the probability that a false positive will occur on at least one platform (and one may be enough to start a war.) For example, if there are 1000 platforms, and each one has a one-millionth (1.000E-6) probability of experiencing a false positive, then the cumulative probability that some platform will do so is 9.995E-4, or .09995%. Looking at the table, I'd say the numbers in the lower right corner are rather disquieting, to say the least.

Now let's look at the false negative case. The table is structured a little differently here. In the false positive case, a single failure is disastrous; in the false negative case, it's not. The probability of a false negative should be many orders higher than that of a false positive, simply because the protections against a false positive will actually enhance the chances of a false negative. This table deals with a 100-platform system (that being the most my binomial coefficient routine can handle).

Pn: .001 .01 .05 .1 .2 .3 .4 .5

N: +								
30 1.	.0000	1.0000	1.0000	1.0000	1.0000	1.0000	1.0000	1.0000
35 1.	.0000	1.0000	1.0000	1.0000	1.0000	1.0000	1.0000	0.9991
40 1.	.0000	1.0000	1.0000	1.0000	1.0000	1.0000	1.0000	0.9824
45 1.	.0000	1.0000	1.0000	1.0000	1.0000	1.0000	0.9991	0.8644
50 1.	.0000	1.0000	1.0000	1.0000	1.0000	1.0000	0.9832	0.5398
55 1.	.0000	1.0000	1.0000	1.0000	1.0000	0.9995	0.8689	0.1841
60 1.	.0000	1.0000	1.0000	1.0000	1.0000	0.9875	0.5433	0.0284
65 1.	.0000	1.0000	1.0000	1.0000	0.9999	0.8839	0.1795	0.0018
70 1.	.0000	1.0000	1.0000	1.0000	0.9939	0.5491	0.0248	0.0000
75 1.	.0000	1.0000	1.0000	1.0000	0.9125	0.1631	0.0012	0.0000
80 1.	.0000	1.0000	1.0000	0.9992	0.5595	0.0165	0.0000	0.0000
85 1.	.0000	1.0000	1.0000	0.9601	0.1285	0.0004	0.0000	0.0000
90 1.	.0000	1.0000	0.9885	0.5832	0.0057	0.0000	0.0000	0.0000
95 1.	.0000	0.9995	0.6160	0.0576	0.0000	0.0000	0.0000	0.0000
100 0	.9048	0.3660	0.0059	0.0000	0.0000	0.0000	0.0000	0.0000

Pn is the probability that a given platform will experience a false negative. N is the minimum number of platforms (out of 100) which respond correctly. The table entries give the probability that at least N platforms respond correctly. For example, if the probability of a given platform experiencing a false negative is 0.1 (10%), then the probability is 99.92% that at least 80 out of 100 platforms respond correctly, 58.32% that at least 90 respond correctly, and so on.

Some of the Pn's and Pp's may strike you as much too high. I don't think so. The two tables were constructed on the simplifying assumption that Pn and Pp are constants; actually, they are reliability functions. The longer a platform is in service, the more likely it is to malfunction. If we assume that the time-to-failure rate of a platform is some form of Weibull distribution $[a*B*t**(B-1) * e^{**}(-a*t**B)]$, then the reliability function is given by Z(t) = a*B*t**(B-1). I did not use this in constructing the tables in order to keep from drowning in figures, and because I don't really know how to choose a, B, and unit t, until we get a history of actual performance (and by then it may be too late...) Suggestions are welcome.

Martin Moore (mooremj@eglin-vax.arpa)

Hazards of VDTs and CRTs

Bernie <<u>ELSPAS@SRI-CSLA.ARPA</u>> Fri 6 Sep 85 15:45:16-PDT

To: RISKS@SRI-CSLA.ARPA

RE: RISKS contribution from friend@nrl-csr (Al Friend, Space and Naval Warfare Systems Command); RISKS-1.6

The 1981 FDA study cited by Friend probably contains much useful (albeit rather "soothing") information about VDT *radiation* hazards (ionizing, RF, and acoustic). One should observe carefully, however, that the quoted material fails to mention other kinds of hazards, nor does its title reflect any others. One should, therefore, not assume that *radiation* hazards are the whole story for VDTs. I would have felt more relieved at the data presented had it included some other, more obvious, risk factors such as visual effects.

In particular, recent studies show that at least two visual effects may be quite important as factors producing severe eye fatigue. The first, visual flicker (resulting from the screen refresh rate), is probably well understood (from extensive psychovisual experimentation in connection with TV viewing). The higher screen refresh rates used on some computer graphic displays seem to minimize this problem. However, 60 fields/sec (50, in Europe) is standard for most personal computers.

[Flicker depends on many factors: rate, ambient light, screen contrast, brightness, subject motion, color, etc. More seems to be known about the conditions for minimal *perceptible* flicker than about those that can produce visual fatigue, eyestrain, headaches, etc. Also, there is a fairly large variation among different subjects even for minimal perceptible flicker, and flicker may be noticeable (and annoying) in the "fringe visual field" (off to the side) even when it is not detectable for the object directly ahead.]

The second factor is connected with the fact that the human eye is not chromatically corrected, i.e., its focal accommodation is different for different colored objects. The result is that when the eye is focused correctly on a blue object, a nearby red object will be slightly out of focus. One study [1] indicates that the discrepancy is about 0.5 diopters (for a viewing distance of 50 cm). According to one report I've seen (sorry, I can't find the reference!), this means that in a multicolored display the eye will automatically be making rapid focus adjustments in scanning the screen. Even worse, the effect can also exist in some monochrome displays, i.e., where the character color (white, say) is achieved by a mixture of two differently colored phosphors separated substantially in wavelength. In the latter situation it appears that (at least for some people) the eye may undergo extremely rapid focus oscillations in the futile attempt to bring both component colors into focus. Quite understandably this may result in severe eye fatigue, even though the subject may not be consciously aware of what is happening. This occurs mostly when the two phosphors radiate nearly

pure spectral lines. Single-phosphor displays and those where the component pure colors are close enough in wavelength seem not be prone to this disturbing effect. I recall seeing the statement that AMBER displays are not objectionable for this reason, and that one nation (Sweden or West Germany, I think) has specified amber displays for extended-time industrial use.

It seems to me that the chromatic refocusing effect is probably the more serious of the two cited, especially on high resolution displays. The fact that it seems not to have been noticed on conventional (analog) color TV displays may be accounted for by their relatively poor resolution (low bandwidth). Thus, the brain expects to see a sharper image on a high-resolution (RGB) display than on a conventional TV (where everything--especially the reds and oranges--is pretty blurred anyway).

In summary, in concentrating on the "serious" potential hazards of X-rays, etc., from VDTs, we should not thereby overlook the more obvious factors concerned with the visual process itself.

1. G.M. Murch, "Good color graphics are a lot more than another pretty display," Industrial Research and Development, pp. 105-108 (November 1983).

Bernie Elspas

[Material inside [...] may be deleted at editor's option. Bernie] [The editor decided to leave it in. PGN]

Viruses, Trojan horses, and worms

"Fred Hapgood" <<u>SIDNEY.G.HAPGOOD%MIT-OZ@MIT-MC.ARPA</u>> Fri 6 Sep 85 22:55:13-EDT

I would like to see a discussion by the members of this list of the degree to which computer users, whether individuals or organizations, are vulnerable to worms and Trojan Horses. These terms, which first appeared in this list in #3, refer to programs designed to inflict some form of unpleasantness on the user, up to and including the destruction of the system. Typically they erase all files in reach. I have read discussion, in Dvorak's column in *Infoworld*, of the possibility that such programs might modify the operating system as well such that when the unfortunate user tries to restore the destroyed files from backup disks, those too would be erased. One can also imagine, vaguely, programs that are insidious rather than calamitious, that introduce certain categories of error, perhaps when strings of numbers are recognized. These might be able to do even more damage over the long run.

There are two issues with these programs. The first is what they might do, once resident. The second is the nature of the vector, to borrow a medical term. Worms can be introduced directly, by 'crackers', or surreptiously, by hiding them inside a legitimate program and waiting for an unsuspecting user to run that program on his system, thus activating the 'Trojan Horse'. The article cited in #3 had to do with a program camouflaged as a disk directory that was circulated on the download BBSs. One could imagine a spy novel devoted to the theme: perhaps it was the KGB, and not Ben Rosen, who provided the money to launch Lotus. Inside every copy of 1-2-3 and Symphony is a worm which, every time it is run, checks the system clock to see if it was later than, say, October 1, 1985. On that date the commercial and industrial memory of the United States dies. The CIA suspects something is up, but they don't know what. Unfortunately the director of the team working on the problem is a KGB mole. Fortunately there is this beautiful and brilliant female computer genius ...

Anyway, I have a specific question: can anyone imagine a circumstance in which a program appended to a piece of text in a system could get hold of the processor? It would appear not, which is a good thing, because if such circumstances did exist, then it would become possible to spread worms by pigyybacking them on a telecommunicated piece of text. The right piece of text -- some specialized newsletter, or even a crazily attractive offer from a 'Computer Mall'-- might find itself copied into thousands of systems. But I am not a technical person, and cannot establish to my satisfaction that such an eventuality is truly impossible.

ls it?

Ke: Viruses, Trojan horses, and worms

Peter G. Neumann <<u>Neumann@SRI-CSLA.ARPA</u>> Sat 7 Sep 85 23:59:24-PDT

To: SIDNEY.G.HAPGOOD%MIT-OZ@MIT-MC.ARPA Cc: RISKS@SRI-CSLA.ARPA

Absolutely not. It is quite possible. However, I can assure you that this issue does not now include a virus -- although some message systems tend to permit you to edit a message before resending it, with no indication that it has been altered. Thus, even in the presence of all of those routing headers, you can never be sure you really have picked up or been forwarded the original message. The example of squirreled control characters and escape characters that do not print but cause all sorts of wonderful actions was popular several years ago, and provides a very simple example of how a message can have horrible side-effects when it is read.

Worms, viruses, and Trojan horses from their technical aspects are probably best discussed elsewhere -- e.g., in SECURITY@RUTGERS. (See also Fred Cohen's paper in the 7th DoD/NBS Computer Security Conference in 1984.) From the RISKS point of view, they are definitely important to this forum -- and they present a very serious risk to the public. PGN]

The Case of the Broken Buoy

Herb Lin <<u>LIN@MIT-MC.ARPA</u>> Fri, 6 Sep 85 16:01:38 EDT

To: mab@RIACS.ARPA cc: risks@SRI-CSL.ARPA

> Did the NWS say that (ie, even if the buoy had been alive at the time, they could not have predicted the storm) in testimony, or after the verdict? If after the verdict, no comment.

I believe it was during testimony, but I am not certain.

But

if as testimony, Herb, the jury (or judge) apparently didn't believe the NWS testimony. If you believe the NWS claim, the headline was correct, but it's unfair to say the court ruled that way when it explicitly based its ruling on negligence.

But it is not clear that the court understands that the significance of "missing data" is context-dependent. Sometimes it matters, and sometimes it doesn't. This is a point that non-scientists have a very hard time understanding.

I am not defending the NWS; they should have repaired the buoy. But given limited resources, how are they to set priorities in deciding what to repair first? The implications of the verdict are to me frightening, placing NWS and all other similar organizations in a double bind: all equipment must be functional even when they don't have sufficient dollars to keep it that way.

×

Matt Bishop <<u>mab@riacs.ARPA</u>> 6 Sep 1985 1359-PDT (Friday)

Cc: risks@SRI-CSL.ARPA Subject: Re: The Case of the Broken Buoy

But it is not clear that the court understands that the significance of "missing data" is context-dependent. Sometimes it matters, and sometimes it doesn't. This is a point that non-scientists have a very hard time understanding.

At this point I'm going to bow out of the discussion, since I am not familiar enough with the decision to know if the court understood that point. The NWS certainly should have made its position very clear, so the court could make an informed decision (about whether or not negligence was involved.)

Re: Hot rodding you AT

Keith F. Lynch <<u>KFL@MIT-MC.ARPA</u>> Fri, 6 Sep 85 09:24:39 EDT

To: RISKS@MIT-MC.ARPA

Date: Wed, 4 Sep 85 14:41:38 EDT From: Dan_Bower%RPI-MTS.Mailnet@MIT-MULTICS.ARPA Subject: Hot rodding you AT

In a recent issue of PC Magazine, Peter Norton espoused the idea of substituting a faster clock chip to enhance performance. Now, according to the folk on the Info-IBM PC digest, this may create problems. An off the shelf PC AT is composed of components guaranteed to work to IBM spec, e.g. 6 Mhz. If I increase the clock rate, then the whole rest of the machine has to be up to snuff. If not, a part dies and I pay a nasty repair bill.

Now if I took Mr. Norton's word as gospel, swapped chips and set my PC AT on fire, would he be liable? How about the publisher?

I doubt this would break anything. The machine would simply cease working above a certain speed, and resume working below that speed.

I know of a couple people who have done this on APPLE computers, tried various speeds so as to run their machine at the highest speed it will go.

Also, I once did the same thing with a synchronous link, i.e. hooked up an external clock and cranked it up to the highest speed it would work reliably at.

Also, I have done this with my Hayes modem. The standard duration for touchtone pulses is 70 ms. The phone system here will accept as short at 38 ms.

...Keith



Search RISKS using swish-e

Report problems with the web pages to the maintainer



Nancy Leveson <<u>nancy@uci-icsd</u>> 08 Sep 85 14:58:56 PDT (Sun)

I had not intended to get involved in the RISKS Forum discussions, but despite my great respect for John McCarthy's accomplishments, I just cannot let his latest message (RISKS-1.8, Sept. 8) pass without comment.

Some important points that need to be considered:

1) Nothing is completely safe. All activities and technologies involve risk. Getting out of bed is risky -- so is staying there. Nitrates have been shown to cause cancer -- not using them may mean that more people will die of food poisoning.

2) Technology is often introduced for the mere sake of using the "latest,"

sometimes without considering the fact that the situation may not really be improved. For example, everybody seems to be assuming lately that machines will make fewer mistakes than humans and there is a frantic rush to include computers and "artificial intelligence" in every new product. Where speed is the determining factor, then they may be right. Where intelligent decision making in the face of unforeseen situations and factors is foremost, then it may not be true. Some electro-mechanical devices may be more reliable than computers. Since I am identified with the area of "software safety," I am often consulted by those building safety-critical software systems. It is appalling how many engineers insist that computers do not make "mistakes" and are therefore safer than any other human or electro-mechanical system. We (as computer scientists) have often been guilty of condoning or even promoting this misconception. Often it seems that the introduction and use of non-scientific and misleading terminology (e.g. "intelligent," "expert", "proved correct") has far outstripped the introduction of new ideas.

3) Technology introduced to decrease risk does not always result in increased safety. For example, devices which have been introduced into aircraft to prevent collisions have allowed reduced aircraft separation with perhaps no net gain in safety (although there is a net gain in efficiency and profitability). There may be certain risk levels that people are willing to live with and introducing technological improvements to reduce risks below these levels may merely allow other changes in the system which will bring the risks up to these levels again.

4) Safety may conflict with other goals, e.g. productivity and efficiency. Technology that focuses on these other goals may increase risk.

John McCarthy suggests that people ignore the risks of not using technology. I would suggest that it is not that these risks are ignored, but that they are known and we have learned to live with them while the risks of using new technology are often unknown and may involve great societal upheaval in learning to adapt to them. Yes, wood smoke may cause lung cancer, but note that recent studies in Great Britain show that the incidence of prostate cancer in men who work in atomic power plants is many times that of the general population. To delay introducing technology in order to assure that greater risks are not incurred than are currently borne by the population seems justifiable. Yes delay may cause someone's death, but the introduction may cause even more deaths and disruption in the long-run.

The solution is to develop ways to assess the risks accurately (so that intelligent, well-informed decision-making is possible) and to develop ways to reduce the risk as much as possible. Returning to the topic of computer risk, citizens and government agencies need to be able to make informed decisions about such things as the safety of fly-by-wire computer-controlled commercial aircraft or between computer-controlled Air Traffic Control with human-assistance vs. human-controlled Air Traffic Control with computer assistance. To do this, we need to be able to assess the risks and to accurately state what computers can and cannot do.

Forums like this one help to disseminate important information and promote the exchange of ideas, But we also need to start new initiatives in computer science research and practice. I have been writing and lecturing about this for some time. For example,

- we need to stop considering software reliability as a matter of counting bugs. If we could eliminate all bugs, this would work. But since we cannot at this time, we need to differentiate between the consequences of "software failures."
- 2) Once you start to consider consequences of failures, then it is possible to develop techniques which will assess risk.
- 3) Considering consequences may affect more aspects of software than just assessment. Some known techniques, such as formal verification and on-line monitoring, which are not practical to detect all faults may be applied in a cost-effective manner to subsets of faults. Decisions may be able to be made about the use of competing methodologies in terms of the classes of faults that they are able to detect, remove, or tolerate. But most important, by stating the "software problem" in a different way (in terms of consequences), it may be possible to discover new approaches to it. My students and I have been working on some of these. Most software methodologies involve a "forward" approach which attempts to locate, remove, or tolerate all software faults. An alternative is to take a backward approach which considers the most serious failures and attempts to determine if and how they could occur and to protect the software from taking these actions.

If using some of these techniques (or despite their use), it is determined that the software would be more risky than conventional systems or is above a minimum level of acceptable risk, then we can present decision makers with these facts and force them to consider them in the decision-making process. Just citing horror stories or past mistakes is not enough. We need ways of assessing the risk of our systems (which may involve historical data presented in a statistically proper manner) and ways to decrease that risk as much as possible. Then society can make intelligent decisions about which systems should and should not be built for reasons of acceptable or unacceptable risk.

Risks of omissions

<<u>Nicholas.Spies@CMU-CS-H.ARPA</u>> 8 Sep 1985 12:00-EST

To: JMC@SU-AI Cc: risks@sri-csl

The question of responsibilities for non-use of computers are largely meaningless in terms of law unless the dangers of non-use were known to substantially increase the probability of greater harm. In the case of your three short examples:

(1) If the ACLU had acted in good faith in seeking to limit sharing of police information and a court had looked favorably on their argument after weighing the possible risks, then the court is responsible because only the

judge had the ability to decide between two courses of action. To make the ACLU responsible would be to deny it and its point of view access to due legal process. To make it necessary for the ACLU to anticipate the court's response to its bringing suit would have the same chilling effect on our legal system.

(2) The same argument applies to the Sierra Club and US 101. If US 101 had been built and then some people were killed, one could as easily conclude that the Sierra Club (or anyone else) might be sued for NOT obstructing the highway!

(3) The "Split Wood not Atoms" poster-vendor might be sued if it could be conclusively proven that he was a knowing party to a conspiracy to give people lung cancer. But we might assume that his motivation was actually to prevent a devastating nuclear accident that might have given 10,000 people lung cancer...

Again, a risks-of-computers organization can only present its case to court and people and, so long as no malfeasance is involved, cannot be held responsible for its failure to predict future consequences. There are far more important "unsymmetric" relationships than that of the press vs. the legal system that pertain to issues of responsibility, namely, that of past vs. future and known vs. unknown. I feel that you are correct in pointing out how computer people would do well to apply their expertise to solving problems of society. In this case the moral imperitives are quite clear.

Kisks of omissions (not using some technology)

Herb Lin <<u>LIN@MIT-MC.ARPA</u>> Sun, 8 Sep 85 15:51:44 EDT

To: JMC@SU-AI.ARPA cc: RISKS-FORUM@MIT-MC.ARPA, risks@SRI-CSL.ARPA

The problem with a forum on the risks of technology is that while the risks of not using some technology, e.g. computers, are real, it takes imagination to think of them....

You raise an interesting point that deserves more discussion. However, as on



Search RISKS using swish-e

Report problems with the web pages to the maintainer



McCarthy, Weizenbaum on SDI

douglas schuler <bcsaic!douglas@uw-june> Mon, 9 Sep 85 09:34:15 pdt

Joseph Weizenbaum states that he would be against SDI "even if it worked." I agree. The premise that "IF the SDI could work, then we must have it (at any price)" is naive. It seems that many people are willing to accept that premise hoping that it will anchor the discussion in the technical area.

One factor which is rarely addressed is that of intermediate systems which the SDI will spawn. There is a tendency to think of the SDI system as being one big system that one day appears overhead as a whole, integrated system. I have little doubt that the SDI plan includes many deliverables along the way. These intermediate systems will both be arguably non-defensive and pose a large problem for integration. I.e., the system must not only be trustworthy when "fully deployed" but at a multitude of intermediate steps. Thus risks will exist in advance of the full delivery (if there ever is to be one).

Another factor is the so-called defensiveness of the system. If two people are armed with guns and one suddenly dons a bullet proof vest this act will be perceived as an offensive act.

Pro-SDI people almost always accuse SDI critics of being politically

motivated. Given the immense (and possibly impossible) technical task of getting the system to work, and the guarenteed proliferation of offensive weapons (designed to penetrate the system), it is very, very difficult for me to believe that the pro SDI folk are not motivated primarily from political (and economic!!) grounds.

- Doug Schuler

Why I'm against even a reliable SDI

Jeffrey Mogul <<u>MOGUL@SU-SCORE.ARPA</u>> Mon 9 Sep 85 16:40:02-PDT

To: risks@SRI-CSL.ARPA

To quote from <u>RISKS Vol 1 #8</u>:

2. I can disagree only with one aspect of Weizenbaum's contribution. He says that he would be against SDI even if it would work, but his arguments mainly show even more reasons why it won't "make nucelar weapons impotent and obsolete." It is probably useless to argue about how we would feel about the system if it would work, but I feel the decision would be much harder to make than it is now. [Dave Parnas]

I think this touches on the crux of the matter: what problem is SDI meant to solve? If we could guarantee that SDI would not only "make nuclear weapons impotent and obsolete", but would in fact reduce the risks associated with war (not necessarily the same thing) then I would not be against SDI. However, I argue (and I suspect this is Weizenbaum's point, too) that an SDI that worked according to the current specification would actually increase risks, even though the system performed "flawlessly".

This is not the place to discuss the strategic implications of SDI, but I think it's important to realize that there are those of us who believe both that SDI is not likely to meet its current specification, nor that it would be a good idea even if it did.

[I] would see some truth in the argument that the non-technological solutions also have a clear risk of failure. [Parnas]

I am afraid that there is no failure-proof solution, technological or not, to the problem of "war". John McCarthy is right that we must compare the risks of the technological solution (e.g., SDI) to its non-use. My fear is that, in this case, the problem is not that the use of technology might fail to solve the problem, but that it might actually make things worse.

Kisk Assessment and Risk Management

Edward V. Berard <<u>EBERARD@USC-ECLB.ARPA</u>> Mon 9 Sep 85 08:16:07-PDT

To: risks@SRI-CSL.ARPA

There has been some discussion of comparing alternative risks on the RISKS mailing list lately. For example, what is the risk associated with the introduction of a new technology versus not introducing the technology? Risk assessment and risk management need not be "guesstimates" nor "a number picked out of the air."

The insurance industry has had to assess and manage risks for years. In fact, they have made quite a science out of these two areas. I would recommend that those who wish to find out more about risk management and risk assessment read:

RISK MANAGEMENT AND INSURANCE, Fourth Edition, by C. Arthur Williams, Jr. and Richard M. Heins, McGraw-Hill, 1981.

Don't let the title put you off. Virtually the entire book is dedicated to risk management, with only a few pages on insurance. You will also find that there are entire professional societies dedicated to managing and assessing risk, e.g., the American Risk and Insurance Association and the Risk and Insurance Management Society.

-- Ed Berard EBerard at ECLB (301) 251 - 1626

Risks in displaying a file containing control characters

Keith F. Lynch <<u>KFL@MIT-MC.ARPA</u>> Mon, 9 Sep 85 00:26:04 EDT

To: LIN@MIT-MC.ARPA cc: Risks@SRI-CSL.ARPA, Security@RED.RUTGERS.EDU

Date: Sun, 8 Sep 85 16:40:44 EDT From: Herb Lin <LIN@MIT-MC.ARPA>

My naive model is that I have a special program that intercepts the raw bit stream that comes in from my communications port. It then translates this into ASCII, and then prints it on my screen.

If this is all that my program does, I can't see what harm can be done.

Several kinds of terminals are programmable from the host, in that certain escape sequences can be sent to them to get them to perform actions such as defining the terminal's function keys.

If a user inserts the appropriate escape sequences in a mail message to his system manager, or into a file which will be displayed by the manager, when the manager reads that mail message it will reprogram a function key on the manager's terminal, which the manager may have programmed to do some common harmless function, to instead do some other command such as give the user unauthorized privileges.

This is a fairly well known bug, and many mail systems are now protected against it, in that they will not transmit any control characters or escape sequences to the terminal.

The moral is that there are many subtle ways to break security, and even things that seem to be quite safe may not really be.Keith



Search RISKS using swish-e

Report problems with the web pages to the maintainer



12 Sep 85 11:11:13 EDT (Thu)

From: John Shore <epi-dc!shore@nrl-css.arpa>

It's tempting to respond to Weizenbaum by arguing against the general proposition, "Don't do it if there's a way around it". After all, should we refuse to develop bullet proof vests and to equip police officers with them just because a criminal might approach from behind and stab them in the ass?

Assuming that a proposed defensive system will work, the relevant question is what is the cost of developing it compared to the cost of getting around it?

In the case of SDI, one should distinguish between defense against a few missiles vs. defense against a massive attack. Either defense would be enormously expensive to develop. If the goal of the attacker is to detonate a few bombs (or threaten to do so), then it is obviously easier and cheaper to get around SDI than through SDI. Here, Weizenbaum is probably right. If the goal is massive or total destruction (including destruction of our missile forces), then getting around SDI (assuming SDI works) does not appear to be either easy or inexpensive. Here, Weizenbaum is probably wrong. In this case, however, the premise is most likely also wrong.

Moreover, suppose that the premise is right -- i.e. SDI works perfectly. As

Parnas has pointed out, there's no way for anyone to establish this fact, which shows the absurdity of arguments like "give us SDI and we will dismantle our missiles".

🗡 SDI

John McCarthy <<u>JMC@SU-AI.ARPA</u>> 12 Sep 85 0057 PDT

To: risks@SRI-CSL.ARPA

Some remarks of mine about SDI on Stanford BBOARD have been referred to. For the benefit of non-readers of that BBOARD, they mainly concerned whether I, like Chris Stuart, should use the IJCAI platform to say something about it. I said nothing in my lecture, but in my press conference, added to my remarks on AI, the remark that there was no principle of computer science that says that programs of any particular task cannot be written and debugged. Not much interest was shown by the assembled press; there was exactly one question on that point.

At the suggestion of Robert Jastrow, who is one of the main scientific defenders of SDI, I made the same point in letters to three Congressmen, said to be influential in the matter of SDI appropriations.

Now I shall say my opinion about SDI.

1. If it can be done, it should. If it affords complete protect, that's great, and if it affords partial protection, that's good. The balance of terror is a bad thing. Here are answers to some counter arguments to its desirability. (a) Joe Weizenbaum says that it attempts a technological solution to a problem that should be solved morally. Alas, moral progress has been so slow that almost the only moral problems to be even partially solved are those that can at least partially been turned into technological problems. For example, the technology of contraception has greatly reduced human unhappiness. (b) It is argued that the Soviets would have to attack at the first sign of deployment. Every past imminent advance by either side has in principle given the other side some temptation to strike before it can be deployed. So far as we know, neither side has even come close to giving in to such temptation. One reason is that the effect of any advance is always subject to a probabilistic estimate, so temporizing has always looked better than attacking. Even if SDI works very well, it may be that no-one will be able to be sure that it is that good.

However, most likely the main reason has been is that neither side ascribes the very worst intentions to the other with certainty. Each side has always said, "Perhaps they don't actually mean to attack us. Why have a nuclear war for sure instead of only a certain probability?" Anyway the Soviets have experienced a period in which we had complete nuclear superiority and didn't attack them.

2. My opinion is that if the physics of the problem permits a good anti-missile defense the programs can be written and verified. However, it

will be quite difficult and will require dedicated work. It won't be done by people who are against the whole project. Computer checked proofs of program correctness will probably play some role. So will anticipating what kind of bugs would be most serious and putting the biggest effort into avoiding them. Having many people go over and discuss all the critical parts of the program will also be important.

More on SDI reliability

<<u>mooremj@EGLIN-VAX</u>> Tue, 10 Sep 85 13:56:45 CDT

To: risks@sri-csl.arpa Cc: soft-eng@mit-xx, lin@mit-mc, mooremj@eglin-vax

> From: Herb Lin <LIN@MIT-MC.ARPA>

> My primary complaint about your otherwise interesting table is that it
> assumes independent failure modes. I think it is much more likely
> that the effects of coupled failures are larger. In particular, given
> the failure of one platform, it is more likely that more than one will
> fail.

Good point. My original post did concern only statistically independent failures. If I can be forgiven one more table, I'll address coupled failures.

Independent failures are caused by events isolated to a single platform, e.g., electrical component failures. The occurrence of such a failure in platform J does not affect the probability of a similar failure in platform K, i.e., $P(K|J) = P(K|\sim J) = P(K)$.

Coupled failures are failures such that the probability of failure is low in any platform, but is greatly increased in all platforms when it occurs in any one of them. For example, consider that a hostile power might develop a new method for its missiles to escape detection. The probability that it will fool any one platform may be low; but if it fools one platform it is likely to fool more than one, perhaps all. For arbitrary platforms J and K, $P(K|J) <> P(K|^J)$.

The original false positive table is not affected by this, since it showed the probability that at least one platform would fail. Coupled failures do not change that probability, only the probability that if one fails, others will (although it is true that while this country might be able to explain away a single false positive, explaining a whole bunch of them could be a lot tougher!)

The false negative case is where the kicker really comes in. The original false negative table applies to independent failures. The following table is structured similarly, but instead of using the probability of failure (Pn), it uses the degree of coupling, Pn(K|J). This table shows, for a 100-platform system, the probability of various numbers of successful responses, given that at least one system has experienced a coupled failure.

Pn(K|J): .5 .6 .7 .9 .95 .99 .8 N: 0 | 1.0000 1.0000 1.0000 1.0000 1.0000 1.0000 5 | 1.0000 1.0000 1.0000 1.0000 0.9746 0.5550 0.0033 10 | 1.0000 1.0000 1.0000 0.9973 0.5355 0.0265 0.0000 15 | 1.0000 1.0000 0.9998 0.9123 0.0677 0.0001 0.0000 20 | 1.0000 1.0000 0.9896 0.5200 0.0017 0.0000 0.0000 25 | 1.0000 0.9993 0.8740 0.1204 0.0000 0.0000 0.0000 30 | 1.0000 0.9822 0.5116 0.0097 0.0000 0.0000 0.0000 35 | 0.9988 0.8525 0.1465 0.0003 0.0000 0.0000 0.0000 40 | 0.9781 0.5054 0.0176 0.0000 0.0000 0.0000 0.0000 45 | 0.8426 0.1574 0.0008 0.0000 0.0000 0.0000 0.0000 50 | 0.5000 0.0219 0.0000 0.0000 0.0000 0.0000 0.0000 55 | 0.1574 0.0013 0.0000 0.0000 0.0000 0.0000 0.0000 60 | 0.0219 0.0000 0.0000 0.0000 0.0000 0.0000 0.0000 65 | 0.0012 0.0000 0.0000 0.0000 0.0000 0.0000 0.0000 70 | 0.0000 0.0000 0.0000 0.0000 0.0000 0.0000

For example, if the degree of coupling is 0.7 -- that is, if something that causes failure in one platform has a 70% chance of causing failure in any other platform -- then the probability is 51.16% that at least 30 of 100 platforms will respond correctly, 14.65% that at least 35 will, and so on, GIVEN THAT THIS TYPE OF FAILURE OCCURS IN THE "FIRST" PLATFORM. Don't forget that the probability that the first platform will fail is UNRELATED to the probabilities in this table!

As far as the relative probabilities of independent and coupled failures, I haven't a clue. The independent failures are the easiest to get a handle on through reliability theory; the coupled failures may be the result of unknown shortcomings in design, or due to unknown hostile actions. (There is an old saying that there are always more unknown errors than known errors, because known errors are limited, but unknown errors are unbounded by definition!)

> Martin Moore mooremj@eglin-vax.arpa



Search RISKS using swish-e

Report problems with the web pages to the maintainer



Charlie Crummer <<u>crummer@AEROSPACE.ARPA</u>> Thu, 12 Sep 85 19:00:29 PDT

>Date: 12 Sep 85 0057 PDT
>From: John McCarthy <JMC@SU-AI.ARPA
>Subject: SDI
>To: risks@SRI-CSL.ARPA

>

>... there [is] no principle of computer
>science that says that programs of any particular task cannot be written and
>debugged.

Computer Science does not contain or deal with the principles operative in the writing and debugging of large, nay, HUGE, eclectic, software programs. This is the realm of Software Engineering. By a similar token there is no principle of the theory of random processes that says that the works of Shakespeare cannot be written by 1,000,000 monkeys pounding 1,000,000 typewriters either, in fact in principle that would be one way of reproducing these works. No serious student of Shakespeare who knew something about random processes would propose such an undertaking, of course. A mathematician who knew nothing about typewriters and little about Shakespeare, however, might if Ronald Reagan pursuaded him that the problem should be worked by assigning 1,000,000,000,000 monkeys to 1,000,000,000,000 typewriters. In software engineering as well as mechanical engineering there is the concept of feasibility to be considered.

> Now I shall say my opinion about SDI.

>

>If it can be done, it should.

If you had a gun wouldn't you be more afraid to face a gunman with a bullet-proof vest than one without? If he began deliberately to put this vest on as he stood before you with his gun leveled at you wouldn't you be inclined to fire before he got the vest on?

>If it affords complete protection that's great, >and if it affords partial protection, that's good.

You speak in the present tense but "it" does not exist! How can a non-existence afford anything? At least one of the basic questions is whether it can be made at all.

>The balance of terror is a bad thing.

Yes, and SDI would only enhance the terror. The "civilized" world has no defensive answer to the terrorists in such mundane places as on airliners, let alone in space, and such is not in the offing.

>Here are answers to some counter

>arguments to its desirability. (a) Joe Weizenbaum says that it attempts a >technological solution to a problem that should be solved morally.

MUST be solved between the terrorizer and terrorizee. When someone's out to get you there's no place to hide. (D. Corleone)

>Alas,

>moral progress has been so slow that almost the only moral problems to be >even partially solved are those that can at least partially been turned into >technological problems.

Not true, viz. cannibalism and slavery.

>For example, the technology of contraception has >greatly reduced human unhappiness.

What evidence do you have of that?

>(b) It is argued that the Soviets would

>have to attack at the first sign of deployment. Every past imminent advance
>by either side has in principle given the other side some temptation to
>strike before it can be deployed. So far as we know, neither side has even
>come close to giving in to such temptation. One reason is that the effect
>of any advance is always subject to a probabilistic estimate, so temporizing
>has always looked better than attacking. Even if SDI works very well, it
>may be that no-one will be able to be sure that it is that good.

You may be safe in saying that but I hope our leaders are not so cavalier. Most serious strategy is based on "worst case" scenarios.

> However, most likely the main reason has been is that neither side >ascribes the very worst intentions to the other with certainty. Each side >has always said, "Perhaps they don't actually mean to attack us. Why have a >nuclear war for sure instead of only a certain probability?" Anyway the >Soviets have experienced a period in which we had complete nuclear >superiority and didn't attack them.

>

>2. My opinion is that if the physics of the problem permits a good >anti-missile defense the programs can be written and verified. However, it >will be quite difficult and will require dedicated work. It won't be done >by people who are against the whole project. Computer checked proofs of >program correctness will probably play some role. So will anticipating what >kind of bugs would be most serious and putting the biggest effort into >avoiding them. Having many people go over and discuss all the critical >parts of the program will also be important. >

Whether the physics of the problem admits a good anti-missile defense is a paramount question. It will take much more than dedicated climbing of the automatic proof of correctness "tree" to get to the "moon" of an "astrodome" over the U.S. a la Reagan's definition of strategic defense.

--Charlie

SDI and Safeguard

John Mashey <<u>mips!mash@glacier</u> > Thu, 12 Sep 85 22:56:02 pdt

I used to work with many of the people at Bell Labs who worked on the Safeguard ABM; they were competent people who knew how to build complex systems. Maybe there were some who believed that it was actually possible to build a reliable, deployable, maintainable ABM that one could expect to work in real use; if so, I never met any; most folks did not so believe, and said so. [They did believe that you could shoot down missiles in well-controlled tests, because they'd done it; they just didn't believe it would work when it needed to.]

SDI and Robert Jastrow

Herb Lin <<u>LIN@MIT-MC.ARPA</u>> Thu, 12 Sep 85 20:08:22 EDT

To: JMC@SU-AI.ARPA cc: LIN@MIT-MC.ARPA, risks@SRI-CSL.ARPA From: John McCarthy <JMC at SU-AI.ARPA>

At the suggestion of Robert Jastrow, who is one of the main scientific defenders of SDI, I made the same point in letters to three Congressmen, said to be influential in the matter of SDI appropriations.

Robert Jastrow is certainly a defender of the SDI, but he has admitted publically in his own Congressional testimony that he does NOT carry out scientific analyses of anything related to SDI. He hardly counts as a "scientific defender."

✓ Some financial disaster cases from Software Engineering Notes

Peter G. Neumann <Neumann@SRI-CSLA.ARPA>

Fri 13 Sep 85 00:22:19-PDT I hope that the RISKS Forum will not degenerate into only an SDI Forum, so I thought I would counterbalance this issue with a new topic. I have resurrected a contribution from the July 1985 SIGSOFT SEN, and also preview some newer cases that will appear in the October 1985 SEN (which is just about ready to go to press). (The few of you who are ACM SIGSOFT members please pardon me for the duplications.)

[FROM ACM Software Engineering Notes vol 10 no 3, July 1985]

Disasters Anonymous 1: A Rose is Arose is (Three) Z-Rose

Now and then I get a story that I cannot print. (I do have a few, but don't ask. I have of course conveniently forgotten them all.) Here, is one that can be printed -- although its author must remain anonymous. Note that the case of the three extra zeroes resulting from two different assumptions about the human interface bears an eerie resemblance in cause to the case of the shuttle laser experiment, which follows after this one. [PGN]

A group within my company had a policy of dealing only in multiples of one thousand dollars, so they left off the last three digits in correspondence to the wire transfer area to make their job easier. Other groups, however, had to write out the full amount since they did not always deal with such nice round numbers. One day, a transaction was processed that had a value of \$500,000. The person who entered the transaction thought that it was from the group who dealt in multiples of \$1000 and entered it as \$500,000. Of course, this was not the case, so a \$500,000 transaction became a \$500,000 one.

The only thing that prevented a disaster was that it was sent to a small company that called back to verify the amount, and the error was then caught. However, this was a Federal Reserve transaction and the funds had been transferred, but the timing was good and the transaction was backed out before it became a disaster. My opinion is that such critical software should have caught the error before the wire was sent to the Federal Reserve.

Another error in a Federal Reserve transfer had to do with multiple transactions per communications transfer. In this case, the Federal Reserve software put a pair of nulls in the data that should have been translated as blanks. However, they were stripped out and a \$200,000,000 incoming wire lost. To maintain the Fed balance, money was purchased to cover a deficit that didn't exist -- since the money was a credit. This was a substantial monetary loss because of inadequately tested software.

[FROM ACM Software Engineering Notes vol 10 no 5, October 1985]

Disasters Anonymous 2: Financial Losses

Our anonymous contributor from SEN 10 3 (July 1985) has come through again.

Since I sent some disaster reports to you in May, another one has occurred. This one caused some financial loss and acute headaches among managers.

Most large banks subscribe to the Federal Reserve's funds transfer system, frequently referred to as "Bankwire". Our system that connects to Fedwire was being upgraded with a new DDA interface to the host to help protect against overdrafts. During a review, it was determined that the software was not quite ready, but should be okay to put into production two days later. I cautioned them against doing so since not all of the bugs had been resolved, and the software had not been "stress tested" (or whatever phrase you wish to use about testing that ensures that it will work in production).

The first day of production went fine. However, the main file in the new software was an ISAM file that had degraded significantly during the first day. On the second day, that file continued to fragment and started to consume a large amount of the system resources. This slowed response time so much that by the end of the banking day, we still had hundreds of wires to send to the Federal Reserve. We had to request extensions every half hour for hours to try and squeeze the transactions through the system so that the money would get to our customers.

In addition, the response-time problem and other bugs in the software prevented us from knowing our Federal Reserve balance. Since we must maintain some 150 million dollars in our Fed "checking account", this lack of information could cause significant financial loss as 1.5 billion dolars were posted that day and we were off by hundreds of millions of dollars at first.

Another part of this disaster is that the slow response time caused one program to assume that the host was down. When a transaction finally went through, our system would transmit the DDA information, but the host did not acknowledge that they already had the wire. Thus a large number of wires were being "double posted" (money sent twice). At the end of the day, tens of millions had been double posted.

As of this writing, the Fed balance had been straightened out, but not all of the double postings had been recovered. Note that at current interest rates, a bank loses \$350 per day per million dollars of unused money.

[FROM ACM Software Engineering Notes vol 10 no 5, October 1985]

Disasters Anonymous 3: Insurance, Reinsurance, and Rereinsurance

Perhaps anonymity is contagious. Re: reinsurance, here is another letter from a different contributor.

I'm newly receiving SEN and found the ``war stories'' quite interesting. Here are three more. I would prefer anonymity should you choose to print these.

This first is hearsay (from a former co-worker). Apparently he and his wife had a joint account with a \$300 balance. They needed \$200 in cash, but due to miscommunication they both made \$200 withdrawals - she at a teller's window (cage?) and he at an ATM (automatic teller machine) - within minutes of each other. When the dust settled they found that their account had a zero balance: the first \$200 withdrawal left a \$100 balance, the second should have left a negative balance of \$100, but the computer generated a \$100 credit to offset the shortfall. The icing on the cake was my friend's inability to explain/convince the bank of this situation and have them accept restitution.

I need to be circumspect about this second story -- it might well have involved fraud. While a consultant, I was hired to review a reinsurance agreement. The reinsurance industry is an old-boys, ``handshake is my bond'' industry as insurors frequently offset their risk by selling it (reinsuring) to other insurors. That is, I insure your building for \$10,000,000 and re-sell all or part of that risk to another firm. Apparently, late one Monday morning (nearly 11:00 a.m. EST), my client got notice across his computer network from another firm that it was reinsuring (i.e. off-loading risk) to my client to the tune of several million dollars. The message was time-dated Friday evening (6:00 P.M., WST). As ``luck'' would have it the property in question had suffered a catastrophic loss over the weekend. The bottom line was that the message had been sent directly (not through any of the store-and-forward services) and the time-date was thus determined by the

clock-calendar on the sender's computer. Need I say more?

Finally, a story told to me ``out of school" by a friend at one of the nation's largest insurance companies. They apparently are involved in so many reinsurance deals that it turned out that they were reinsuring themselves. I.e., Jones reinsured with Smith who reinsured with Brown who reinsured with White who reinsured with Smith. Smith, it turned out was paying both Brown and White commissions for accepting his own risk. The computer system was not designed to look beyond the current customer, neglecting the loop.



Search RISKS using swish-e

Report problems with the web pages to the maintainer



NONCONVERGENT ITERATIVE LOOP. LET'S TRY TO STICK A LITTLE MORE TO COMPUTER-RELATED ISSUES, ALTHOUGH I RECOGNIZE THAT THE TECHNICAL ISSUES MAY BE OVERWHELMED BY NONTECHNICAL ISSUES. BUT PLEASE DO NOT INTERPRET THIS AS AN ATTEMPT TO SQUELCH MEANINGFUL DISCUSSION. PGN ***]

Wire-Transfer Risks; Risk of Non-application of Technology

Saltzer@MIT-MULTICS.ARPA Fri, 13 Sep 85 10:51 EDT

Re: Wire-Transfer Risks

- The current (September, 1985) issue of IEEE Communications magazine on page 23 suggests that it may be typical in the wholesale financial business to carry transactions in thousands of dollars rather than in (ones of) dollars. If so, you would think that the people responsible for software in that business would check and recheck their specs and the human engineering across those interfaces where dividing or multiplying by 1000 is a possibility, wouldn't you?
- 2. The comment that current money prices lead to losses of about \$350 per day for each mislaid million dollars seems to have been intended to suggest that such mistakes are unacceptable. The people in the wholesale money movement business draw an opposite conclusion: since they can quantify their exposure so precisely, they can decide rationally when the loss rate has become unacceptable and it is thus worth paying someone to develop a more error-free system. (For the price of a contract to SRI to develop a verified 1000-line program one could probably afford to mislay IBM's entire revenue stream for a week.)

Re: Risk of Non-application of Technology

For another economically quantifiable example, the early reports on the creation of the SABRE airline reservation system by American Airlines explicitly mentioned a business decision, with two alternatives: invest in two more Boeing 707's, or in developing SABRE. The first approach provided more spare seat-mile capacity that could thus be managed with less precision; the second offered the hope of better management of available seat-mile capacity. Two other considerations that were explicitly mentioned were the cost of customer disatisfaction when reservations were dishonored (accidental overbooking, as contrasted with intentional overbooking, was a rampant problem at the time) and the cost to the company in lost revenue if the prospective computer were to go down for several hours or if the entire contents of the disks were lost. The decision to develop SABRE thus represents an example of up-front assessment of the risk of nonapplication of technology, compared with the risk of applying it.

Model Date-Time stamps (and errors therein)

TMPLee@MIT-MULTICS.ARPA Fri, 13 Sep 85 12:15 EDT

It was an interesting coincidence that the latest Risks_Forum had a piece related to the correctness of the time-stamp on messages. About two days ago I logged on late (about half-past midnight, Central time) and started going through my electronic in-basket. One of the messages struck me: its header was time-stamped 03:56 EDT -- how could I possibly be reading it two and a half-hours before it was sent? (yes, the dates were right -- it wasn't from the previous night/early-AM.) Eventually got a copy of the original from its author. The key to the mystery is that Multics does a timezone conversion on most (but not all) time fields in incoming message headers. The original message's time-zone was clearly marked as PDT, so multics dutifully added three hours and gave me the time in EDT. When we (I and a multics guru) first looked at just the multics version we speculated that perhaps multics had taken the message's time-zone as GMT, which I think would have given the same result. I also thought perhaps since the original was before midnight and the result after, that might have been the cause. In the process of writing this entry for the Risks forum I looked at the original message one more time, and it struck me: for some reason the ISI clock had been set to run on Eastern Time (00:56) but the ISI mailer software (or something else there) thought it was keeping Pacific, hence the PDT tag. What was further confusing was the fact that I looked at several other messages from ISI from about the same period (two to four days ago) and some came out right and some not. Sounds like a good ingredient for a mystery story, at least.

// JMC's remarks

Joseph Weizenbaum <JOSEPH@MIT-XX.ARPA> Fri 13 Sep 85 12:57:15-EDT

Contrary to John McCarthy's inference that I hold to the "general proposition, 'Don't do it if there's a way around it'", I think that proposition to be (even purely logically) absurd. The "way around it" would be another "it" to which the rule would apply, and so on.

Another instance of John putting words in my mouth I didn't (and wouldn't) utter is his "Joe Weizenbaum says that [SDI] attempts a technological solution to a problem that should be solved morally". He makes it easy for himself to score a point by pointing to the slowness of "moral progress" and so on. I believe I wrote that SDI is a technological fix for a problem that is primarily political, cultural, economic, and so on, and that it has to be attacked in these contexts, that we must actually confront the problem of how peoples who organize their societies differently from one another can peacefully share the same globe. That is considerably different from saying the problem should be "solved morally". The trouble with technological fixes is often, and I think in this case, that they give the impression the problem has been dealt with and that no further efforts to deal with it are necessary. In the present instance the spread of such an impression with respect to the peaceful coexistence of the Western and the Eastern block nations could be fatal to the whole world.

Subjective Factors in Risk Assessment

moorel@EGLIN-VAX Fri, 13 Sep 85 13:48:04 CDT

There is a very interesting article about various types of risks and the way that people perceive them in the October issue of _Science_85_. In particular, it makes a couple of points that I feel are quite relevant to this forum's discussions. First, that people respond to risks differently depending on whether the risk is presented as a positive or a negative risk. "Because losses loom larger than gains, we are more willing to gamble to avoid them." Second, it points out that most people are less concerned and aware of the risksof things over which they feel that they have some control. "If we can't be certain about the risks we face, we at least want to have some control over the technologies and activities that produce them."

When we look for examples of the risks of using computer technology vs. the risks of not using computer technology, we ought to keep these two ideas in mind, and ask ourselves whether we are being truly objective about the risks involved or are we letting other, subjective factors influence our judgement. I recommend this article for your reading.

Lynne C. Moore (MOOREL AT EGLIN-VAX.ARPA)

Moral vs. Technological Progres

Charlie Crummer <crummer@AEROSPACE.ARPA> Fri, 13 Sep 85 10:56:21 PDT

> From: McNelly.OsbuSouth@Xerox.ARPA

> In-Reply-to: NEUMANN%SRI-CSLA:ARPA's message of 13 Sep 85 01:19:23 PDT

> (Friday)

<>>Alas,

<>>moral progress has been so slow that almost the only moral problems to be
 <>>even partially solved are those that can at least partially been turned into
 <>>technological problems.

<>Not true, viz. cannibalism and slavery.

> Actually, it's my understanding that the demise of slavery was due to

> technological advances which made slavery economically unfeasible. The

> invention of the cotton gin, for example, made it only a matter of time

> here in the US before slavery died out. As far as cannibalism goes, I'd

> say that was more caused by Western culture steam-rolling over the

> cannibals.

> -- John --

Actually McCarthy's original comment presupposes that moral and technological progress are comparable. It is that assumption that I disagree with. Ethics and the attendant morality provide the context within which all activity, and in particular technological progress, exists. Morality and technology are not substitutes for one another and moral progress is not dependent on technology nor vice versa. There is always technological progress attendant to moral progress just because there is always technological progress.

--Charlie



Search RISKS using swish-e

Report problems with the web pages to the maintainer



Peter G. Neumann <Neumann@SRI-CSLA.ARPA> Sat 14 Sep 85 23:18:42-PDT

The text of the message that follows this one is taken verbatim from the HUMAN-NETS Digest (HUMAN-NETS@RUTGERS), 11 Sep 1985, Volume 8 : Issue 29, on the topic of risks in EMAIL. That topic is of vital significance to the RISKS Forum, for at least two reasons:

- (1) You should recognize the risks that might be incurred by you in submitting messages to this forum, and in sending on-line messages in general.
- (2) The free propagation of messages not copyrighted can itself lead to significant risks to the contributor and to the RISKS Forum, if those messages were false or libelous, or if they are altered.

In general, you and I must assume that any message on this forum may be forwarded indefinitely and read by anyone, and could appear in print in all sorts of strange places. (If something worthy of inclusion in the ACM Software Engineering Notes is at all controversial, I ask for explicit permission before publishing it.)

What is even RISKIER is that your message can be trivially altered along the

way as it traverses the network of networks, possibly drastically changing your intended meaning. Use of check sums and crypto seals can reduce the risk of undetected alteration, but does not solve the problem entirely.

Peter G. Neumann

(This message is not copyrighted.)

preserving rights to Email messages.

Larry Hunter <Hunter@YALE.ARPA> Tue, 3 Sep 85 11:08:31 EDT

Copyright-by: Larry Hunter, 1985

After consulting with several lawyer friends, the conclusion I reach is that anything you send out over the nets is public property -- ie, anyone can reproduce it verbatim, for profit and the author has no right to control its use. There is, however, a very simple way to preserve the author's rights to control the use his messages are put to. The courts have held that practically any clear attempt of an author to preserve his/her rights to a written work are sufficient to actually preserve them. No need to add the 'circled c' to ASCII, just add a 'Copyright-by:' line to the header of your local mailer and voila! your rights are preserved.

Larry

PS. I am not a lawyer and this is only my opinion - if you have a vital interest in some related matter, talk to a real lawyer!

Kisk Comparisons

<TTussing.es@Xerox.ARPA> 13 Sep 85 13:27:12 PDT (Friday)

Someone sent me this and I thought the people on this mailing list might be interested.

Excerpt from a pamphlet by Dow Chemical Corp, entitled Life is in the Balance:

Dr. richard Wilson, who is professor of physics at Harvard, has devised a mathematical formula that measures risks in terms of the minutes and seconds of life lost. Taking the average person of 30 who has a life-span in the United States of approximately 73 years, Wilson says that statistical person cuts time from his life in the following ways:

Smoking one cigarette - minus 12 minutes Drinking a diet soft drink - minus about 9 seconds Driving without a seat belt - 6 seconds for each trip Being an unmarried male - minus 1800 days Being male rather than female - minus 2700 days

We can also view risks by figuring which risks are qeual. For example, the following items all pose an equal risk of increasing the likelihood of death by one chance in a million:

Drinking half a liter of wine Spending three hours in a coal mine Living two days in New York Traveling six minutes by canoe Riding 10 miles on a bicycle Driving 300 miles in a car Flying 1000 miles by jet

Kisks history/philosophy

<Nicholas.Spies@CMU-CS-H.ARPA> 14 Sep 1985 01:06-EST

This is definitely old news, but then again the facts behind the case have only recently seen the light of day. In his recent biography "Alan Turing: the enigma" (Simon & Schuster) Andrew Hodges reveals in some detail the inner workings of the German Enigma encryption device (arguably a "computer") which contributed (backhandedly) to the development of computers as we know and love them today. (If you're interested in Turing, computers or WWII history read it, if you haven't already.)

The portion of the book devoted to Turing's stint at Bletchley Park is peppered with lost opportunities on the German side. Apparently with little additional effort the Germans could have rendered the "Bletchley bombes" completely useless. In fact the only reason the Germans were not careful was their unswerving faith in the Enigma device. Even when there was ample evidence pointing to a message-security problem the integrity of Enigma was never seriously questioned by the Germans. There were, of course, countless other factors, but the German faith in their technological answer was in large measure responsible for their losing the U-boat war and very likely the war itself.

Another anecdote, not related to computers (recounted in either "The Ultra Secret", Winterbotham or "Bodyguard of Lies", A. Cave Brown, two other excellent books on the secret war) gave one reason for the German atomic bomb project not really getting off the ground. It seems that a German professor of the old school was in charge of finding a material for moderating a chain reaction (by absorbing neutrons). Graphite was tried but failed which meant that deuterium (heavy water) was thought to be needed. When it was suggested that the graphite might not be pure enough (which, as it turned out, was the reason the test failed) the professor reacted with rage that his authority was being questioned and he effectively derailed German research in reactor design. (Later the plant for making heavy water built in Norway was sabotaged by British agents which made a reactor impossible which preventing the manufacture of fissile material.)

These examples suggest that excessive reliance on either technological solutions or "authoritative opinion" may carry grave risks, albeit in these cases for an evil regime. The question facing us is whether we (or the Soviets, for that matter) have fallen into the same traps. I would say that we (both) definitely have, for the means to power are now more than ever technological (as opposed to political or diplomatic) and one or another "expert" is routinely trotted out to "prove" the efficacy of this or that technological scheme.

Indeed, how can it be otherwise? Hitler opened the Pandora's Box of applying high-tech to warfare and it worked (at least until a higher-tech response prevailed). After WWII a new era was born in which global political power no longer rested on moral authority but on a command of the new applied sciences and scientists. Engineers had provided political leaders with instruments of war for centuries, but now scientists are looked upon as the fountainhead of political power, by dictators, politicians and the people alike. It may now be said truly that Knowledge is Power.

To some the risks of technology are the inevitable consequence of the inexorable "progress" that technology itself represents. It seems to me that this view places too great an emphasis on the growth of "technology" itself at the expense of our ability to integrate it with human wants and needs. It's almost to say that "technology" has a virtual life of its own that we have no control over. This is manifestly untrue because "technology" is the mere summation of the creative acts and compulsions of a great number of people enamored of the idea of "technology". But if "technology" does have a life of its own it must be based on a willing denial of responsibility on the part of each member involved in furthering it, particularly when large populations or the world are put at risk by introducing a new "technological development". It seems, therefore, self-evident that morality and technology are intimately interwoven.

In the largest sense, the risks of computers are the risks of having an increasing number of computer experts that are in a position to tell people what computers can be safely used for. Their expert opinions may be well thought out or erroneous, as the case may be, but they are in fact the only opinions that the public, financial institutions, military establishments or politicians can depend on. The fact that any or all may place a value on this expert information and act on it puts a heavy moral burden on the providers of this information, whether they like it or not.

The only population that I have had direct contact with who have faced this primal issue of the risks of technology are the Amish-Mennonites of Ontario; I made a film about their 150th Anniversary in Canada. (I have also edited films about the Amish in Lancaster Co., PA.) The trigger for the Amish was rubber-tired wheels on carriages around the 1870's because this allowed the young of courting age to "go to town" more easily, with a perceived disruption of Amish life not far behind. To this "improvement" they said "No". Subsequently, the Amish have taken great care to keep the increasing technological developments surrounding them at bay, but not by pure rejection. In short, they have evaluated the risks of adopting technologies.

For instance, gasoline engines are permitted for stationary use (and also on horse-drawn wagons) for harvesting, threshing, bailing and for powering milk refrigerators. There's no contradiction in using a valuable power source so long as it isn't applied to providing the means for increased contact with the outside world. Electricity is used if generated within the farm; and public telephones may be used as well; as long as wires (i.e. connections) to the outside world are avoided there is no reason to avoid using the technology. The oddity of the Amish is based on common sense when their objectives are known.

Although the Amish reaction to technology may strike many as merely "quaint" they do show that it is possible to stop short the "inevitable" growth of technology. (The Amish are renowned for their success in farming, which is not the case for many others that have embraced modern technological ways.)

I am not advocating a general return to Amish ways (indeed this only makes sense within the context of Amish values), but I will say that we all face a similar confrontation with a technology that may do us great harm on many fronts. Unfortunately we are prone to treat our own creations (be they buildings, cars, chemicals or computers) as if they are as benevolent as the products of 5 billion years of co-adaptive evolution. As increasingly complex and interdependent as our creations become, the more they will reveal themselves as ill-suited to the tasks they were meant to perform; it only stands to reason because of the lack of a truly global feedback in the design process. And also, how are we to judge the efficacy of our machines if we have lost sight of the reason we have created them?



Search RISKS using swish-e

Report problems with the web pages to the maintainer



Peter G. Neumann <<u>Neumann@SRI-CSLA.ARPA</u>> Mon 16 Sep 85 20:25:57-PDT

To: RISKS@SRI-CSLA.ARPA

After reading the case of the double posting of hundreds of millions of dollars in **RISKS-1.11**, some of you apparently experienced the multiple posting of RISKS-1.13 -- all original mailings time-stamped Sat 14 Sep 85 23:43:07-PDT, all complete, and all identical. Brint Cooper, for example, received THREE identical copies at various time intervals.

Received: from brl-aos.arpa by TGR.BRL.ARPA id aa20274; 15 Sep 85 3:23 EDT Received: from sri-csl.arpa by AOS.BRL.ARPA id a017885; 15 Sep 85 3:18 EDT

Received: from brl-aos.arpa by TGR.BRL.ARPA id a021160; 15 Sep 85 4:47 EDT Received: from sri-csl.arpa by AOS.BRL.ARPA id a018065; 15 Sep 85 4:35 EDT

Received: from brl-aos.arpa by TGR.BRL.ARPA id a022055; 15 Sep 85 6:31 EDT Received: from sri-csl.arpa by AOS.BRL.ARPA id a018257; 15 Sep 85 6:17 EDT

The new


Report problems with the web pages to the maintainer



One of the more interesting sessions at the 8th International Conference on Software Engineering was a discussion of software for the Strategic Defense Initiative (SDI). The moderator was Manny Lehman and the panelists were Fred Brooks, David Parnas, and Alan Perlis. The discussion was originally intended to be a debate, but Fred Brooks was not willing to participate in a debate because he had not yet reached a resolution of the issues. (I understand that volunteers for the position of opposing Parnas in a debate on SDI were hard to find. Dr. Brooks deserves credit for being willing to engage in a public exploration of touchy issues about which he feels unsettled in concert with a strongly opinionated colleague in an effort for both audience and panel to learn more.)

The discussion started with a presentation by Parnas of the technical reasons why reliable SDI software cannot be built. (Readers of this newsletter will be familiar with many of the arguments put forth by Parnas. A complete discussion in hard-copy is available from him at the University of Victoria, Department of Computer Science, P.O. Box 1700, Victoria, B.C., Canada.)

Brooks responded with reasons why he thought we could build such a system. His major point was that we have built similar systems in the past. He identified the Apollo missions software as an example, suggesting that we start with such a system and incrementally build from it towards an SDI system, using what's learned along the way.

Perlis then added a few comments, explaining why SDI software would be more complex than existing software and why it is of the hardest type of software to build. His argument was that the SDI system represents a moving target in terms of requirements and design.

Following some further discussion among the panelists the floor was opened to technical questions from the audience.

The major place in which Parnas and Brooks seemed to disagree was whether or not similar systems have been built. Brooks tried to use the Apollo and Space Shuttle as examples. Parnas's point was that in those systems everything can be predicted in advance. In an anti-missile system, the number, shape, and trajectories of launched missiles can't be predicted. In addition, the system must distinguish decoys from real warheads. Finally, the defense system itself will be under attack. As a result, realistic tests and simulations of operating conditions for such a system could not be conducted.

All the discussants seemed to agree that an SDI system could not be built error-free, and that it would not be completely reliable. Nonetheless, there were advocates of building it on such grounds as that it would only be needed for a short time, and could be turned off the rest of the time, or that we now place our trust in systems that are also untested and probably unreliable.

In summary, there were no good responses to any of the questions that Dave Parnas raised. Nonetheless, there were arguments put forth for the construction of an SDI system on the grounds that it need not be completely reliable.

David Weiss Wang Institute of Graduate Studies

Kisks to the Moderator!

Peter G. Neumann <Neumann@SRI-CSLA.ARPA> Thu 19 Sep 85 17:40:08-PDT

To: RISKS@SRI-CSLA.ARPA

<u>RISKS-1.15</u> was ready to go out Wednesday night. Murphy hit in spades. The SRI MICOM switch for dial-up access was unavailable for two days, and is still down. An alternative route might have been available through the only system that receives dial-ups directly from a split-speed modem, but that

system went down for five hours. Several other more circuitous alternative routes all ran into broken gateway, which resulted from a power failure Tuesday night. It would not have helped to drive back to SRI, because the SRI-CSLA (which kept running through all this) was out of net contact as a result of a gateway problem. All of the gurus were invisible. If you ever get this issue, you will know that things have improved. Peter



Search RISKS using swish-e

Report problems with the web pages to the maintainer



<<u>WAnderson.wbst@Xerox.ARPA</u>> 18 Sep 85 15:48 EDT

Courtesy-of: minow%rex.DEC@decwrl.ARPA (Martin Minow, DECtalk Engineering)

FROM AIList Digest Friday, 20 Sep 1985 Volume 3 : Issue 125

At the recent IJCAI at UCLA I picked up a couple of papers at the GE exhibit booth. One of these, entitled "A Tutorial on Expert Systems for Battlefield Applications," (delivered at a meeting of the Armed Forces Communications and Electronics Association last May) states that "AI systems that incorporate human expertise may be the only way" to fill the gap between availability of people and complexity of military hardware. In defense of this strategy the author states:

- In contrast with humans, AI systems are good at handling the myriad details of complex situations, such as often occur in military settings.

- In contrast with other computational approaches that are more formal

and algorithmic, AI systems are more robust: they are designed to deal with problems exhibiting uncertainty, ambiguity, and inaccuracy.

I find it appalling (and frightening) that statements like this can be presented in a technical paper to military personnel. The author (according to the references) has contributed widely to the AI field at many conferences. It's simply ludicrous to state that current AI systems are better in battlefield situations than humans. What was the last AI system that could drive a tank, carry on a conversation, and fix a broken radio whilst under enemy fire? The second comment is equally misleading. To contrast "formal and algorithmic" with "robust" seems to imply that algorithms and formal procedures are inherently not robust. On what is this claim based? (There is no reference attached to either statement.) It sounds like a recipe for unreliable software to me.

How can someone write this stuff? I know, to make money. But if this is the kind of information that is presented to the military, and upon which they make decisions, then how can we expect any kind of fair assessment of the possible projects in the Strategic Computing (and Defense) Initiatives? How can this kind of misinformation be rebutted?

Bill Anderson

P.S. The full reference is available on request.

🗡 RISKy Stuff

<<u>PADLIPSKY@USC-ISI.ARPA</u>> 20 Sep 1985 18:33:30 EDT

To: neumann@SRI-CSL.ARPA

... I suppose I might as well succumb to temptation and offer a couple of comments on stuffgoneby:

The most striking omission, to my mind, in the SDI discussion is (unless I missed spotting it) the failure to draw the parallel to SAGE. For those who don't remember/know, the Semi-Automated Ground Environment was the grandfather of the big, "man-machine" system, certainly in DoD and most probably in the field as a whole. It was intended to allow for the interception of manned bombers. It is widely acknowledged to have spun off a lot of what became the state of our art (collective art, that is-- i.e., what I call the computer racket). Like SAGE, SDI is probably dealing with the wrong threat (since things don't have to go through the air to go boom ... and since things don't even have to go boom to rack up megadeaths). Also like SAGE, SDI might have useful spinoffs (a 20-years-younger colleague claims to be for it because it should help get him off this planet). Unfortunately, unlike SAGE it seems to possess a real potential for stampeding the presumed Bad Guys into doing something ... unfortunate.

What a good thing we Men of Science know better than to reason

from analogy, eh?

... muted cheers, map

Mailer Protocol Woes

Rob Austein <<u>SRA@MIT-XX.ARPA</u>> Fri, 20 Sep 1985 14:36 EDT

I was actually a culprit in a similar mailer lossage earlier this week. The whole thing actually started out when I was dialed up to XX on a noisy connection. Improbable as it seems (although not quite on the order of monkeys and Shakespeare), the random line noise managed to generate the 7 character command sequence necessary to send off my entire mail file as a single message to a major mailing list. All 110 pages (=281600 bytes) worth of it. Fortunately for the network (but unfortunately for my reputation) the list happened to be the TOPS-20 maintainers' mailing list, so the message got killed off in pretty short order. I have since put in a couple of safeguards into my mail reader environment so that this particular lossage can't happen again, but since the real culprit was transmission line noise I have been kind of nervous about reading my mail over dialups ever since....

--Rob

Kisks in Synchronizing Network Clocks (RFC956 Now Available)

<> 25 Sep 1985 09:07:47 PDT

From: Ann Westine <WESTINE@USC-ISIB.ARPA> Plucked-From: Request-For-Comments-List: ;

A new Request for Comments is now available from the Network Information Center in the <RFC> directory at SRI-NIC.ARPA.

RFC 956:

Title:Algorithms for Synchronizing Network ClocksAuthor:D. L. MillsMailbox:Mills@USC-ISID.ARPAPages:26Characters:68868

pathname: <RFC>RFC956.TXT

This RFC discussed clock synchronization algorithms for the ARPA-Internet community, and requests discussion and suggestions for improvements. The recent interest within the Internet community in determining accurate time from a set of mutually suspicious network clocks has been prompted by several occasions in which errors were found in usually reliable, accurate clock servers after thunderstorms which disrupted their power supply. To these sources of error should be added those due to malfunctioning hardware, defective software and operator mistakes, as well as random errors in the mechanism used to set and synchronize clocks. This report suggests a stochastic model and algorithms for computing a good estimator from time-offset samples measured between clocks connected via network links. Included in this report are descriptions of certain experiments which give an indication of the effectiveness of the algorithms. Distribution of this memo is unlimited.

Public access files may be copied from the <RFC> directory at SRI-NIC.ARPA via FTP with username ANONYMOUS and password GUEST.

The normal method for distribution of RFCs is for interested parties to copy the documents from the NIC online library using FTP. Requests for special distribution should be addressed to either the author of the RFC in question or to NIC@SRI-NIC.ARPA. Unless specifically noted otherwise on the RFC itself, all RFCs are for unlimited distribution.

Submissions for Requests for Comments should be sent to POSTEL@USC-ISIB.ARPA.

Requests to be added to or deleted from this distribution list should be sent to NIC@SRI-NIC.ARPA.

--jon.

[I include this item in the RISKS Forum for a very obvious reason: one of the nastiest of all problems in distributed computer systems and networks is the synchronization problem. That so many seemingly correct algorithms have in fact been flawed is a very important consideration here. PGN]

Ke: Moral vs. Technological Progress

<>

Wednesday, 25 Sep 1985 16:27-EDT

X-From: joel@peora.UUCP (Joel Upchurch)

>Actually McCarthy's original comment presupposes that moral and >technological progress are comparable. It is that assumption that I >disagree with. Ethics and the attendant morality provide the context >within which all activity, and in particular technological progress, >exists. Morality and technology are not substitutes for one another >and moral progress is not dependent on technology nor vice versa. >There is always technological progress attendant to moral progress >just because there is always technological progress.

I don't think that there is any such thing as an absolute moral standard. Morality is simply a set of customs that evolves by trial and error to improve the survival chances of the social group (family, tribe, nation whatever). Notice that this has has little to do individual survival and that a moral principle, such as patriotism, may cause the individual to get killed.

Now I think it fairly easy to see that the capacity to put group survival ahead of self-interest is an important genetic trait and that tribes of people that had this trait would be more likely to survive that tribes that didn't. That is not to say that this moral capacity doesn't vary greatly from one person to the next or that even that it may not be more fully realized in one person than another because of upbringing. It is even possible that, because of some genetic error, some people may be born without a moral capacity, just like they might be born without arms or legs.

The point I'm trying to make is although there will always be these survival customs we call morality, the nature of the customs is heavily dependent on the context they evolve in. Thus the morals of a herding society may be greatly different from those of an agrarian one. Even two societies in similar contexts may evolve different moral solutions to the same problems. This implies that if the context in which a society operates changes, then the morals of that society will have to change too. In recent centuries the most important changes in the social context have been caused by technology. Thus the morals appropriate to a agrarian society are not always appropriate to an industrial one or those of an industrial society to a post-industrial one.

Moral progress means the evolution of survival customs more appropriate to the current context. The trouble in recent centuries has been that our ability to evolve new technology has outstripped our capacity to evolve the appropriate morality for it. There is a strong tendency to stick to the morality that one learns as a child, even if it not appropriate to the current situation.

Our current problem is that we have a technology that supplies us with ICBMs and a morality that includes national patriotism. Now it is obvious to any thinking person that this is a serious dilemma. Some people argue that we should adopt a new morality, more appropriate to this technology, and indeed in the long term they are correct, although one can argue what is the most effective moral solution to this problem.

The trouble is that moral solutions evolve slowly. Even today much of our morality is left over from our nomadic and agrarian heritage and has limited relevance in our modern society. In order to apply the long term solution, we must first survive in the short term, and in that short term technical band-aids, like the SDI, are appropriate. Technology put us into this situation and I don't see why we can't ask technology to assist us in the solution. To think that we can solve the problem by an overnight revolution in human nature is wishful thinking of the most dangerous sort.

Joel Upchurch

Perkin-Elmer Southern Development Center 2486 Sand Lake Road/ Orlando, Florida 32809/ (305)850-1031 {decvax!ucf-cs, ihnp4!pesnta, vax135!petsd}!peora!joel

Kisk Contingency Planning -- Computers in Mexico

Mike McLaughlin <<u>mikemcl@nrl-csr</u> > Sat, 21 Sep 85 13:25:25 edt

This is not info, but a call for info. I have no idea how bad the computer bug has bit in Mexico, but the current news & TV coverage of the disaster suggest that whatever computing/networking is going on must have been affected. If any RISKS reader knows some statistics or details about computer usage in Mexico, and can give insights as to what happened, what backup and alternative modes were in place, how well they worked... etc. It would certainly help me, and perhaps many others in planning for the disaster that we hope never comes. Perhaps we could discuss just what we want to find out, and then go after the answers formally, if there are no informal contacts on the net. - Mike

[This item may seem a little odd for the RISKS Forum, but when you realize that Mike's Navy job involves expecting the unexpected risks in computer and network usage, and planning what to do, it is indeed relevant. By the way, in Mexico, as usual in times of disaster, the ham-radio buffs lept in to help. Computer networks and internets also have a role to play. I'm ready with my battery-operated portable terminal. (This issue is being sent from DC.) PGN]



Search RISKS using swish-e

Report problems with the web pages to the maintainer



SDI debate announcement

<<u>genrad!teddy!lkk@mit-eddie.MIT.EDU</u>> 26 Sep 1985 17:48-EST

To: risks@sri-csl.arpa

Dear Colleague,

Computer technology plays an ever-increasing role in the arms race. The Strategic Defense Initiative ('Star Wars') is a leading example of a military system in which almost complete reliance will be placed on computerized decision making. The feasibility and desirability of this system are currently undergoing serious public debate.

On Monday, the 21st of October, at 8:00 pm in M.I.T.'s Kresge Auditorium, the M.I.T. Laboratory for Computer Science and Computer Professionals for Social Responsibility are co-sponsoring a public forum designed to raise many of the technical issues surrounding the Strategic Defense Initiative (SDI).

Professor Michael Dertouzos, Director of the M.I.T. Laboratory for Computer Science, will moderate a debate on the feasibility of software development for the SDI project. Dr. Danny Cohen (Director of the Systems Division at the University of Southern California's Information Sciences Institute and Chairman of the Strategic Defense Initiative Organization panel on Computing in Support of Battle Management (SDIO/CSBM)) and Professor Charles Seitz (Professor of Computer Science, California Institute of Technology and member, SDIO/CSBM)) will speak in favor of the SDI proposal. Professor David Parnas (Lansdowne Professor of Computer Science, University of Victoria, Canada) and Professor Joseph Weizenbaum (Professor of Computer Science, Massachussetts Institute of Technology) will take the position that such a software development project is infeasible.

Professor Parnas' resignation from the SDIO/CSBM panel in June of this year, and the set of memos he wrote discussing the infeasibility of the SDI project attracted extensive press coverage in June of this year.

CPSR will be holding a reception for the speakers at La Groceria (853 Main Street in Cambridge) between 6:30 and 7:30. Please join us for dinner and an opportunity to meet some of the panelists. The \$25 per plate donation will help us cover expenses for this forum and related projects. Please RSVP to Mark Vilain at (617) 648-4325.

Earlier that afternoon, the M.I.T. Technology and Culture Seminar will sponsor a talk by Dr. James Ionson, Director of the Office of Innovative Science and Technology for the SDIO. After Dr. Ionson describes the general research goals of SDI, two M.I.T. professors will respond with varying views on why they have chosen to accept or refuse funding for research from the SDIO. A student representative will report on student reaction to Star Wars projects on campus. This talk will be held at MIT in building 9, room 150 at 4:00 p.m.

Minor risk to the pocket book

Eugene Miya <<u>eugene@AMES-NAS.ARPA</u> > 26 Sep 1985 1652-PDT (Thursday)

Here is a minor man-machine risk which occurred today (9/26) in the Silicon Valley at El Torito [popular Mexician food chain] at lunch. We arrived for a late lunch and found that our bill was 50% over what appeared in the menu. The cash register [one of those computer systems where they press buttons rather than prices] was running on the dinner menu prices rather than the lunch menu prices. Since we arrived late, everybody else [e.g., hundreds of people] were over-charged for lunch that day and perhaps earlier. This implies several things about the way customers in Si Valley treat their bills [rich? no verification? ...] What about the restaurant?

From the Rock of Age Home for Retired Hackers:

--eugene miya, NASA Ames Research Center, eugene@ames-nas.ARPA

Ke: Technology and Morality

Benjamin Thompson <munnari!mulga.oz!bjpt@seismo.CSS.GOV > Fri, 27 Sep 85 12:01:18 EST

Organization: Computer Science, University of Melbourne

Nicholas Spies writes [in RISKS-1.13]:

Hitler opened the Pandora's Box of applying
 high-tech to warfare and it worked (at least until a higher-tech response
 prevailed).

Technology has been successfully applied to warfare for millenia. Alexander the Great didn't win through having a bigger army (he didn't); he had better weapons (e.g. he found out that ballistae propel spears faster than people do). (and he had better trained soldiers etc. - education and technology basically).

After WWII a new era was born in which global political power no
 longer rested on moral authority but on a command of the new applied
 sciences and scientists.

Nothing could be further removed from morality than the way in which global political power is grabbed and maintained. It has always been based upon physical strength (which usually, but not always, corresponds to technological strength). History is a never-ending sequence of examples.

Social Impacts of Computing: Graduate Study at UC-Irvine

Rob-Kling <<u>Kling%UCI-20B@UCI-ICSA</u>> 26 Sep 1985 0920-PDT

To: risks@SRI-CSL

CORPS: Graduate Education in Computing, Organizations, Policy, and Society at the University of California, Irvine

This graduate concentration at the University of California, Irvine provides an opportunity for scholars and students to investigate the social dimensions of computerization in a setting which supports reflective and sustained inquiry.

The primary educational opportunities are PhD concentrations in the Department of Information and Computer Science (ICS) and MS and PhD concentrations in the Graduate School of Management (GSM). Students in each concentration can specialize in studying the social dimensions of computing.

The faculty at Irvine have been active in this area, with many interdisciplinary projects, since the early 1970's. The faculty and students in the CORPS have approached them with methods drawn from the social sciences.

The CORPS concentration focuses upon four related areas of inquiry:

- 1. Examining the social consequences of different kinds of computerization on social life in organizations and in the larger society.
- 2. Examining the social dimensions of the work and organizational worlds in which computer technologies are developed, marketed, disseminated, deployed, and sustained.
- 3. Evaluating the effectiveness of strategies for managing the deployment and use of computer-based technologies.
- 4. Evaluating and proposing public policies which facilitate the development and use of computing in pro-social ways.

Studies of these questions have focussed on complex information systems, computer-based modelling, decision-support systems, the myriad forms of office automation, electronic funds transfer systems, expert systems, instructional computing, personal computers, automated command and control systems, and computing at home. The questions vary from study to study. They have included questions about the effectiveness of these technologies, effective ways to manage them, the social choices that they open or close off, the kind of social and cultural life that develops around them, their political consequences, and their social carrying costs.

CORPS studies at Irvine have a distinctive orientation -

- (i) in focussing on both public and private sectors,
- (ii) in examining computerization in public life as well as within organizations,
- (iii) by examining advanced and common computer-based technologies "in vivo" in ordinary settings, and
- (iv) by employing analytical methods drawn from the social sciences.

Organizational Arrangements and Admissions for CORPS

The CORPS concentration is a special track within the normal graduate degree programs of ICS and GSM. Admission requirements for this concentration are the same as for students who apply for a PhD in ICS or an MS or PhD in GSM. Students with varying backgrounds are encouraged to apply for the PhD programs if they show strong research promise.

The seven primary faculty in the CORPS concentration hold appointments in the Department of Information and Computer Science and the Graduate School of Management. Additional faculty in the School of Social Sciences, and the program on Social Ecology, have collaborated in research or have taught key courses for CORPS students. Our research is administered through an interdisciplinary research institute at UCI which is part of the Graduate Division, the Public Policy Research Organization.

Students who wish additional information about the CORPS concentration should write to Professor Rob Kling (Kling@uci-icsa), Department of Information and Computer Science, University of California, Irvine, Irvine, Ca. 92717, 714-856-5955 or 856-7548, or Professor Kenneth Kraemer (Kraemer@uci-icsa), Graduate School of Management, University of California, Irvine, Irvine, Ca. 92717, 714-856-5246.

Friendly enemy test teams

John Mashey <<u>mips!mash@glacier</u> > Wed, 25 Sep 85 01:17:53 pdt

John McCarthy <JMC@SU-AI.ARPA> writes in RISKS-1.10:

> 2. My opinion is that if the physics of the problem permits a good
> anti-missile defense the programs can be written and verified. However, it
> will be quite difficult and will require dedicated work. It won't be done
> by people who are against the whole project. Computer checked proofs of
> program correctness will probably play some role. So will anticipating what
> kind of bugs would be most serious and putting the biggest effort into
> avoiding them. Having many people go over and discuss all the critical
> parts of the program will also be important.

Perhaps the best way to make it work WOULD be to have a test team of people (who might be skeptics, at least) trying to break it. Most large complex projects that actually worked, at least that I've seen, have succeeded at least partly because they had a large test team who didn't believe anything worked until it could get past the worst of their tests. I don't know what the ratio is elsewhere, but many complex ATT/BTL projects allocated 30-50% of the staff to building test frameworks designed to stress the system under test. Consider the recent history of evaluation of new military systems (like the Sergeant York). It's very hard for the builders of something to evaluate it well; you need a good enemy for that.

[Tiger teams have indeed had some success in finding the more obvious program bugs, but in general many flaws may remain. This topic has been raised superficially in past issues. Perhaps we are ready for some detailed discussions on the strengths and limitations of testing. PGN]

More protocol goofs

Dave Curry <<u>davy@purdue-ecn.ARPA</u> > Thu, 26 Sep 85 22:29:41 EST

[The original message contained 8576 characters, almost exclusively headers. I have pruned it to give just the flavor. PGN]

I'm forwarding this as a wonderful example of protocols getting completely hosed... this mail of mine bounced for some unexplained

reason. I resent the message the same day this came back, and it went through just fine.

Looking at the headers should make the problem more than obvious...

--Dave Curry

id AA24764; Thu, 6 Sep 84 02:25:55 edt Received: by mcnc (4.12/4.7) id AA00613; Wed, 5 Sep 84 18:51:54 edt Original-From: <unc!unc!unc!unc!unc!unc!unc!mailer-daemon@mcnc>

[... and so on iteratively, ad nauseum, down to...] Received: by unc (4.12/4.7) id AA06045; Wed, 5 Sep 84 09:07:16 edt Original-From: <mailer-daemon@mcnc> Received: by mcnc (4.12/4.7) id AB15479; Wed, 5 Sep 84 08:01:18 edt Date: Sat, 1 Sep 84 10:03:51 est Original-From: Mail Delivery Subsystem <MAILER-DAEMON@mcnc> Subject: Returned mail: Unable to deliver mail To: mcnc!mcnc!unc!mcnc!unc!mcnc!unc!mcnc!unc!mcnc!unc!mcnc!pur-ee!davy@unc

----- Transcript of session follows -----554 sendall: too many hops (30 max)

----- Unsent message follows -----

[...]

[I am reminded of the tale of the unattended British power station equipped with an automatic calling unit to report troubles. When it finally had to dial the emergency reporting number, it received a recorded message that the number it had dialed was not valid. PGN]



Search RISKS using swish-e

Report problems with the web pages to the maintainer



* Lack of a backup computer closes stock exchange

<<u>mooremj@EGLIN-VAX</u>> Mon, 30 Sep 85 11:44:49 CDT

To: risks@sri-csl.arpa

When Hurricane Gloria was approaching the New York area, the New York and American Stock Exchanges did not open. The Midwest Exchange, located in Chicago, opened on schedule; unfortunately, it had to close 40 minutes later, when its nationwide computer system failed. Where is the central computer of that system located? New York, of course. The Director of the Exchange was quoted as saying, "Well, this has got to change."

✓ DPMA survey on computer crime offenses

Jan Lee <<u>janlee%vpi.csnet@CSNET-RELAY.ARPA</u>> Wed, 2 Oct 85 15:39 EST

Peter ... here are the proper figures on Computer Crime Offenses as reported by the DPMA from a survey taken by COMP-U-FAX (TM) and reported 1985 May 27:

(It doesn't say how many people were surveyed -- just that DPMA is an organization of 50,000 members.)

21% reported one or more abuses in past 3 years in their workplace. 2% of these offenses were committed by outsiders (so much for the Hacker myth!!). The reasons for the abuses were:

27% ignorance of proper professional conduct26% playfulness25% personal gain22% maliciousness

Only 45% of respondents worked for a company who had a full-time or part-time data security person.

Only 2.2% of abuses were reported publicly (does that mean reported to the news media or the legal authorities?).

The surveyor was Detmar Straub, Grad. School of Business Admin., Indiana University.

(In a note I got from Donn Parker, Donn seems to cast some aspersions on the validity of this survey, but I haven't had chance to do anything other than read the press release myself.)

JAN

Ethics vs. morality

Marty Cohen <<u>mcohen%NRTC@USC-ECL.ARPA</u>> Fri, 27 Sep 85 13:18:47 PDT

"Morals: Society's code for individual survival" "Ethics: An individual's code for society's survival"

From Theodore Sturgeon, "More Than Human" ("Baby is Three" is one part of the book), page 177 of the Ballentine books paperback.

Mathical Man-Month of Risk

Stavros Macrakis <<u>macrakis@harvard.ARPA</u> > Thu, 3 Oct 85 19:14:56 EDT

In reference to the discussion on the Wilson article: > ... formula that measures risks [as] ... seconds of life lost ...

In discussing risks, whether from computer systems or other causes, it would surely be desirable to have some reasonable guidelines. Wilson's basic point was that we should be able to calculate costs and benefits; a point with which I am in fundamental agreement. However, this calculation has many difficulties. In this note, I should like to sketch (in a somewhat disorganized way) some of these difficulties.

It is often useful to reduce complicated facts to simple unidimensional measures for comparison. But such reduction loses a great deal of information in general; and also ignores variation in personal utility functions. For that matter, statistical measures should differentiate between associations and causation.

Among the figures cited, there were several misleading measures along these lines.

For instance, although perhaps cigarette smokers ought to allocate 12 minutes of their lives per cigarette, a lung cancer death is typically far harder than an automobile accident death. On the other hand, car accidents subtract years by killing fewer, younger, people; cancer by killing more, but older, people. How to compare 5 x (lifespan 25-70) with 25 x (lifespan 63-70)? Is each 175 man-years? I have no answer, although I have certain intuitions--in particular, 'losing' the 69 man-years 1-70 seems far less tragic than losing the 69 man-years 3 x (47-70) ('struck down in the prime of life'): but the Wilson extract did explicitly talk only of 25+-year-olds. Economics has various answers: discounted productivity contribution; market value attached to hazardous jobs; None is satisfactory, but all are useful for separating grossly different risks.

As for correlations, why is it that living in New York is hazardous? Perhaps it is the pollution. But if it is the poverty or the street crime, then poverty or bad neighborhoods (regardless of city) probably relate far better statistically and surely causally than does residence. New York just has many poor people and bad neighborhoods. A statistical analysis that excludes such correlated hazards is surely non-trivial.

`Post hoc ergo propter hoc' seems especially implicated in the case of unmarried males. There are likely advantages to being married, but perhaps inability to find or keep a wife indicates other problems.

Then there is the presumption of linear additivity. Even the risks which are not strongly correlated may combine: consider asbestosis and smoking.

Of course, in other cases the unidimensional metrics may be far more useful. In the case of the costs of unreliable funds transfer, the cost to the bank can be calculated quite precisely. In cases where these errors affect customers, it may also be reasonable to estimate that damage (e.g., you may lose \$100 of annual profits per error of type X if a retail customer takes his business elsewhere). If you're a materials supplier to a just-in-time manufacturer, the monetary consequences may be far more serious: still, a monetary measure may be meaningful.

In conclusion, it seems to me useful to develop a range of measures of cost

and benefit, and not try to reduce them to single numbers. If one wishes to be ultra-cautious, one will then weigh the minimum expected benefit against the maximum expected cost. If one is a `rational' gambler, perhaps the average benefit against average cost. If one is an optimist or a gambler, perhaps the maximum benefit against the minimum cost. I believe Howard Raiffa (among others) discusses such issues (although I'm afraid I can't provide a reference).

Risk-free systems are unlikely. We need good ways of evaluating risks and benefits.

-S

Date: Sat, 28 Sep 85 16:05:48 edt From: mikemcl@nrl-csr (Mike McLaughlin) To: RISKS@SRI-CSLA.ARPA Subject: Risk Assessment by real people

Ellen Goodman's column in The Washington Post, Saturday, 28 Sep 85, (c) 1985, The Boston Globe Newspaper Company, is worth reading. Title is: "AIDS: The Risks We'll Take." No, it doesn't mention computers. It really isn't much about AIDS, either.

What it is about is people, and how risks are assessed by real people - not by computers, or calculators, but by the folks that would die of boredom reading this forum... or might die of something else if *we* do not understand how *they* evaluate risks.

"In California, members of a family cut back on sugar in the decaffeinated coffee they drink in their house - on the San Andreas fault."

"Another friend drinks only bottled water these days, eats only meat untouched by steroids and spends weekends hang-gliding."

"The AIDS story... is a tale about experts and the public, about the gap between our skepticism and our longing for certainty."

Ms. Goodman also quotes an article in October's Science '85: "We may be much more willing to accept higher risks in activities over which we have control, such as smoking, drinking, driving or skiing, than things over which we have little control, such as industrial pollution, food additives and commercial airlines."

Her summation is very relevant to *us*, who read and write about SDI, the use and non-use of computers, and so on: "This is, after all, a country that bans saccharin and builds nuclear bombs. We argue and will go on arguing about risk in two different languages: numbers and emotions, odds and anxieties."

If *we* cannot make ourselves understood by *them* when we discuss what matters for the survival of *all of us*, then this forum is just a modern form of omphaloskepsis.

- Mike

CRTs again, solution to one eye-problem

Mike McLaughlin <<u>mikemcl@nrl-csr</u> > Sat, 28 Sep 85 16:25:57 edt

CRTs can cause eye strain in users who wear glasses. Distance lenses won't focus at closer than arm's length. Reading lenses focus too close. Bifocals require you to hold your head in one of two specific positions... neither of which works. What to do?

I already done it. Several years ago. So much a part of my computerized life that I didn't think of it while reading/writing via computer about CRT usage. Got "intermediate lenses" - an Rx for glasses optimized for my CRT/ VDT viewing habits. Got comfy in front of the tube & keyboard, had a friend measure distance from bridge of nose to CRT screen. Averaged several tries. Gave the distance to my opthamologist - he turned out an Rx in short order.

Bought frame & lenses. Expensive. Use them *only* at office computer - don't take them home (don't have a computer at home). Declared them as a non-reimbursed business expense. IRS content, helped reduce cost.

Did NOT get tri-focals, because:

1. They force you into an even more rigid head position - and I believe that rigid posture is a major cause of computer-fatigue.

2. They confused the IRS issue, which was quite clear with intermediateonly glasses.

3. I'm not old enough to wear TRI-focals, for heaven's sake!

Suggestion:

Employers requiring use of CRT should consider paying for intermediates; should resist paying for trifocals (or even the incremental cost of tri- over bi-focals).

An acceptable alternative might be bifocals, distance/intermediate or intermediate/reading, depending upon the user's eye condition and job content.

- Mike

Failure of Mexican Networks

Shadow <<u>Z.HXWY-FLORY-DAVID%CRNL20A.BITNET@UCB-VAX.Berkeley.EDU</u>> Wed 2 Oct 85 13:43:03-EDT

To: Risks@sri-csl.arpa

This doesn't refer to computer networks, but it is similar.

According to Fred Goldstein on Telecom Digest (Telecom-Request@MIT-MC.ARPA), phone service from most of the world to Mexico City was destroyed by the collapse of the building containing the switches, frames, etc. for Mexico

City's international gateway switch.

Sites which are major network nodes collapsing due to earthquake/etc could result in a similar effect.

David Flory

ARPANET ---> flory@CORNELL-GVAX.ARPA or shadow@RU-AIM.ARPA BITNET ----> z.hxwy-f@CRNL20A.BITNET

[Good engineering tends to avoid sensitivity to single-point failures and to avoid singly connected nodes. Designing for massive failures and disasters is of course much more difficult. PGN]

✓ Technical Reports Lists

Laurence Leff < leff%smu.csnet@CSNET-RELAY.ARPA> Fri, 27 Sep 85 13:38:21 cdt

To: [... all sorts of lists...]

[Here is what could be a useful service if suitable indexing occurs. I have stripped Laurence's message down. SEND to him for the original. This is of course more general in scope than just RISKS, but seemed worth including. -- in case you missed it elsewhere. Respond to him, not me. PGN]

I have volunteered to organize an electronic mechanism for the distribution of technical report lists from Universities and R&D labs. Some (and hopefully all) of the people producing technical reports would send a copy of the list to me. I would then send these to a moderated group on USENET as well as a mailing list for those sites on the INTERNET who do not get news (ARPANET, CSNET, etc.).

I need two things from you:

- 1) if your organization prepares technical reports and sends them out to interested parties (perhaps for a fee), please arrange to have electronically readable copy of your lists sent to trlist%smu@csnet-relay.
- 2) if people at your organization would like to receive lists of tech reports produced by universities and R&D labs, please provide me an electronic address to send them to (if you are not on USENET). Send such administrative mail to trlist-request%smu@ csnet-relay.



Report problems with the web pages to the maintainer

The Risks Digest Volume 1: Issue 18



✓ Emanations and interference in the civil sector

Peter G. Neumann <<u>Neumann@SRI-CSLA.ARPA</u>> Sun 6 Oct 85 15:16:38-PDT

To: RISKS@SRI-CSLA.ARPA

I have had several queries about risks in the civil sector concerning electronic emanations from and electronic interference upon computer systems and networks -- and of course also about what can be done to protect oneself or one's company. For example, Martin Lee Schoffstall

✓ Emanations and interference in the civil sector

Saltzer@MIT-MULTICS.ARPA <<u>lerry Saltzer</u>> Fri, 4 Oct 85 18:02 EDT

To: Neumann@SRI-CSL [in response to a query]

Concern for Electromagnetic Compatibility is indeed beginning to become an important design consideration in consumer products. These days, TV sets are beginning to clean up their act, but the average FM tuner just can't

cope with being in a substantial RF field. As consumers start to collect a walkman, TV, cable converter, FM tuner, stereo amplifier, VCR, CD player, cordless phone, remote control light switches, microwave oven, and garage-door opener under one roof, more and more people are becoming aware of the problems, and discovering that some manufacturers didn't put the right effort in.

Administrivia -- Escaped Mail and Delays

Mark S. Day <<u>MDAY@MIT-XX.ARPA</u>> Thu 3 Oct 85 20:07:38-EDT

[Excerpted-From: Soft-Eng Digest Sat, 5 Nov 85 Volume 1 : Issue 34]

XX was a victim of Hurricane Gloria; it had multiple head crashes when it was restarted after the storm. The heroic efforts of the staff here brought the machine back to life after a marathon of restoring files, which unfortunately left the alias for this list in a strange state. Instead of going into my mailbox, everything sent to "Soft-Eng" was immediately redistributed. Fortunately, only one message got out between the time XX came up and the time I noticed the problem. Anyway, sorry for the difficulties. No doubt this will now appear in the RISKS mailing list as an example of an unreliable computer system...

[SURE. WHY NOT??!! Recovery and reinitialization are a vital part of keeping a system running properly. How many times have you put in a patch or fix only to find that it somehow disappeared, e.g., not surviving a crash or not getting propagated back into the source code? But in this case you got left in an unsafe state! PGN]

✓ Computer databases

<<u>Andy_Mondore%RPI-MTS.Mailnet@MIT-MULTICS.ARPA</u>> Sat, 28 Sep 85 16:20:46 EDT

One topic I have not seen discussed here is that of computer databases. I am Systems Coordinator for the Registrar's Office here so I am in charge of a fairly large database containing (obviously) student grade and course information as well as addresses, demographic information, etc. I'd like to see a discussion of the risks of having incorrect information in a database, information being seen or accessed by the unauthorized individuals, etc. Thanks.

[Ah, yes. This is a wonderful topic. The state of the art of database management systems that can handle sophisticated privacy/compromise and data integrity problems is rather abysmal. However, the risks of people gleaning information by drawing inferences from a database are considerable. For starters, see Dorothy Denning's book, Cryptography and Data Security, Addison Wesley, 1982. As to risks, Software Engineering Notes has had a bunch of stories on the effects of misuse or mininterpretation of police data. The Air New Zealand catastrophe was an example of what can happen if a change is not propagated properly. As always, contributions are welcome. PGN]

Re: Friendly test teams

John Mashey <<u>mips!mash@glacier</u> > Sat, 28 Sep 85 22:31:18 pdt

It might be good to ask for pointers to published data on bug histories, effort levels, robustness in large hardware/software systems. I suspect these may be hard to find for SDI-like systems; I couldn't dig up any old Safeguard info. Although not in the same class of difficulty, ATT's new #5 ESS switch is fairly complex (300+ engineers). A good reference is: H.A. Bauer, L.M. Croxall, E.A. Davis, "System Test, First-Office Application, and Early Field Experience", ATT Technical Journal, vol 64, No 6, Part 2 (Jul-Aug 1985), 1503-1522.

Re: CRTs again, solution to one eye-problem

Brint Cooper <<u>abc@BRL.ARPA</u>> Sun, 6 Oct 85 12:59:18 EDT

[We started out keeping one eye on this problem, but it does not want to stay out of sight. Will this be the last message? PGN]

A cheaper but similar solution was suggested by my opthalmalogist when I attained that stage of life wherein my arms are too short.

Since I needed a small, positive correction (about +1.0) in each eye, I purchased, at his suggestion, "reading glasses" from the local pharmacy for about \$12.00. Since then, my eyes have worsened a little and I need about +1.25 to +1.5 diopters for reading. But this is too strong for the terminal (an AT&T 5620 with rather small font), so I retained the old +1.0 diopter lenses for the terminal at work. At \$12.00 each, I can afford to have a pair at the office, a pair at home, and a pair to carry.

Note: This won't work if one has astigmatism or if one needs widely different corrections in each eye. But ask your doc. You can buy a lot of OTC glasses for \$200.

Oh yes, it is a small nuisance to switch glasses from terminal lenses to reading lenses, but one learns quickly to minimize the hassle.

Brint



Search RISKS using swish-e

Report problems with the web pages to the maintainer



Bill Keefe <<u>keefe%milrat.DEC@decwrl.ARPA</u> > Tuesday, 8 Oct 1985 07:26:03-PDT

I don't know who to credit with typing this in. I was going to summarize, but it's too easy to take some points out of context. It brings up many questions as to who bears the responsibility (liability?) to protect people from such occurrences.

In The Lion's Cage" [Forbes Oct. 7, 1985]

On July 21, 1984, at about 1 p.m., a worker at Diecast Corp. in Jackson, Mich. found Harry Allen, 34, a diecast operator pinned between a factory pole and the back of an industrial robot. But Allen's co-worker couldn't come to his aid. Using the robot's controller, the company's director of manufacturing finally unpinned Allen, who was alive but in cardiac arrest. He died in a hospital five days later.

Allen had entered a restricted area, presumably to clean up scrap metal from the floor. While there, he got in the way of the robot's work, and thus became the first - and so far only - U.S. victim of an industrial robot-related

accident.

That's not a bad safety record, considering that 17,000 robots are now installed in the U.S. But the bet is he won't be the last. The Japanese, who lead the world in robot installations, also lead in robot-related fatalities: There have been reports of at least 5, and possibly as many as 20, such deaths in Japan.

That's only fatalities. In this country, companies are not required to report injuries related to specific equipment, so no reliable data are available. But in Sweden, a pioneer in the use of industrial robots, one study estimates that there is 1 accident a year for every 45 robots. By 1990, when the number of robots installed in American Industry could climb as high as 90,000, the number of injuries could climb accordingly. That's because robots move quickly and are programmed to go through a series of motions without stopping. A worker who gets in the way can be struck, pushed aside, crushed or pinned to a pole as Allen was.

How will industry minimize the risk to its workers? Probably with difficulty. Robots don't easily accommodate safeguards. Whereas most machinery operates within a fixed set of boundaries, robots have a large "striking distance" - the reach of their mobile arms within three dimensions. In automotive assembly plants, maintenance workers often collide with robots adjacent to the ones they're servicing because they don't realize they are in another robot's work area. A robot may perform one task five times and then start on a completely different activity, and with it a different set of motions. Also, a robot can sit idly for a time and then come to alive again, threatening injury to a worker who mistakenly thought it was shut down.

What's being done to make robots safer? Right now, not much. "The extent of most safety precautions are signs saying, 'Restricted Area: Keep Out,' or maybe a guardrail," says Howard Gadberry of the Midwest Research Institute in Kansas City, Mo. Indeed, the most common safeguards - perimeter barriers such as guardrails and electric interlocked gates, which automatically shut down the robot when opened - don't protect those maintenance workers and programmers who must enter the lion's cage. Presence-sensing devices, such as pressure-sensitive mats and light curtains, both of which automatically cut off a robot's power, also don't seem to offer as much protection as is needed, if only because workers are even more unpredictable in their movements than robots. They may not step on the mat when feeding parts to a robot, or they may not break a light curtain's beam.

That's not to say that robots can't be made safer. Researchers at the Renssalaer Polytechnic Institute, for example, recently completed a research prototype for several large U.S. companies of a four-sensor safety system that continuously monitors the area around a robot. Using ultrasonic, infrared, capacitance and microwave sensors, the RPI system is designed to stop a robot in its tracks if a worker gets too close. Cost? Five thousand dollars in production, according to Jack Meagher, a senior project manager at RPI.

The National Bureau of Standards has also been working with ultrasonic sensors on robot arms similar to the system at RPI. They both have developed a secondary, or watchdog, computer to monitor the actions of the robot and its microprocessor. After all, if the robot's computer goes berserk, how can it monitor itself? That's more important than you might think, 30% of robot accidents seem to be caused by runaways, according to John Moran, director of research at the National Institute for Occupational Safety & Health.

While such systems slowly make the transition form research to the factory floor, industry is trying to put basic safety standards into practice. Recently, the Robotic Industries Association proposed a set of national safety standards for robots that could go into effect as early as next summer.

Would such standards have prevented Harry Allen's death? Maybe not. The robot at the Diecast plant was surrounded by a safety rail with an electric interlocked gate that automatically shut down the robot when the gate was opened. However, there were two gaps in the rail that allowed workers to easily bypass the safeguard; that has since been corrected by the company.

Says Allan Harvie, deputy director of the Michigan Department of Labor's bureau of safety and regulation, "I could only presume Harry Allen thought he could go in and do what he intended to do without having to shut the robot down."

Ke: Computer databases

Matt Bishop <<u>mab@riacs.ARPA</u>> 8 Oct 1985 1123-PDT (Tuesday)

I guess I'll start the ball rolling on this discussion.

I think the greatest risk is not from the technological end but the human end. For instance, there was a case a couple of weeks back where someone got stopped for a traffic ticket. Call this gentleman John Lee Jones (I've forgotten his real name.) A routine computer check showed James Lee Jones was a fugitive from an LA warrent, and the description of James Lee Jones was pretty close to what John Lee Jones looked like. So the SFPD hauled him downtown, and ran a fingerprint check to see if there was anything else they could find out about John Lee Jones. Turned out he had used several aliases in the past -- so the SFPD notified the LAPD they had arrested James Lee Jones, and would the LAPD please come up and get him? The LAPD obliged, took him down to LA, and notified the prosecutors.

Throughout all this, Mr. Jones was (vehemently) denying he was James Lee Jones. About a week after he had first been locked up, his public defender persuaded the judge to order the police to compare John Lee Jones' fingerprints with James Lee Jones' fingerprints. They didn't match. End of case.

What's so surprising is that the people throughout the whole proceeding did not question whether the data the computer gave them was relevant. True, it was accurate (so far as I know.) But it was used incorrectly. In other words, in this case the technology didn't fail; the human safeguards did. (Incidentally, in defense of the police, when this came out an investigation was begun to see why the fingerprint comparison was not made immediately; according to police procedure it should have been.) And no amount of database security can guard against this type of breach of security.

[Caveat -- I read the newspaper story I outlined above a couple of weeks ago in the S.F. Chronicle. I have undoubtedly misremembered some of the details, but the thrust of it is correct.]

Matt Bishop

[Add that to the database-related cases of false arrest reported in RISKS-1.5. PGN]

Kegistrar's databases

<<u>Murray.pa@Xerox.ARPA</u>> Tue, 8 Oct 85 06:59:25 PDT

To: RISKS@sri-csl.arpa

Just mentioning grades, computers and risks, all in the same paragraph instantly brings to my mind visions of hackers who are flunking freshman English smiling anyway, knowing that they have figured out how to get an A.

I've always assumed that everybody "knew" that students and grades couldn't really coexist on the same machine. Does anybody know of a school brave/silly enough to do it?

It seems like a great opportunity for somebody who makes a secure system to get a LOT of publicity, one way or the other. Has anybody ever been confident enough to try it? What happened?

Changing the topic slightly... Security on an ethernet is clearly non-existent unless you encrypt everything you care about. Our personnel people upstairs take the problem seriously. The solution is simple. They have their own section of coax. It's not even gatewayed to the rest of our network.

Matabase risks - census data

<<u>Murray.pa@Xerox.ARPA</u>> Tue, 8 Oct 85 07:15:28 PDT

To: RISKS@sri-csl.arpa

The census bureau distributes their data broken down to quite small areas. I don't know the details, but I'm pretty sure it gets down to "neighborhood" sized regions, and it may even get down to the block. When the sample size gets small enough, there are obviously opportunities for gleaning non-statistical information by using carefully crafted querys to read between the lines.

I remember somebody telling me that they worked pretty hard to make sure this couldn't happen. Anybody know what they actually do? Is it written up someplace? Does it work well enough? Any war stories? Are the techniques simple once you know the trick?

[As I noted in <u>RISKS-1.19</u>, Dorothy Denning's book is a good source. The Census Bureau tries to add phony data that preserves all of the overall statistics but that prevents inferences... PGN]

* The winners of evolution...

William McKeeman <<u>mckeeman%wang-inst.csnet@CSNET-RELAY.ARPA</u>> Tue 8 Oct 1985 10:00:15 EST

To: risks@sri-csl

A recent submission included the following paragraphs on evolution of morals...

Now I think it fairly easy to see that the capacity to put group survival ahead of self-interest is an important genetic trait and that tribes of people that had this trait would be more likely to survive that tribes that didn't. That is not to say that this moral capacity doesn't vary greatly from one person to the next or that even that it may not be more fully realized in one person than another because of upbringing. It is even possible that, because of some genetic error, some people may be born without a moral capacity, just like they might be born without arms or legs.

Moral progress means the evolution of survival customs more appropriate to the current context. The trouble in recent centuries has been that our ability to evolve new technology has outstripped our capacity to evolve the appropriate morality for it. There is a strong tendency to stick to the morality that one learns as a child, even if it [is] not appropriate to the current situation.

Evolution is being used with its Darwinian meaning but with an interpretation that includes the more ordinary progress of mankind. The central mechanism of evolution is the failure of the less successful forms to reproduce -- often for failing to live long enough. Evolution is never fast enough to avoid bloodshed -- it is bloodshed that activates it. Until disaster strikes the adapted and unadapted survive undifferentiated.

My point is that if we treat the present sad state of affairs as a problem in evolution rather than politics or technology, we are implicitly planning on rebuilding a world with the (apparently) adapted survivors of WWIII.

W. M. McKeemanmckeeman@WangInstWang Institutedecvax!wanginst!mckeeman

 Image: Tyngsboro MA 01879

 Image: Tyngsboro Tyngsboro Tyngsbor



Public Accountability

Jim Horning <<u>horning@decwrl.ARPA</u> > 10 Oct 1985 1244-PDT (Thursday)

It has now been more than a year since the ACM Council passed its resolution on computer systems and risks to the public. Quoting from RISKS-1.1:

The second part of the resolution includes a list of technical questions that should be answered about each computer system. This part states that:

While it is not possible to eliminate computer-based systems failure entirely, we believe that it is possible to reduce risks to the public to reasonable levels. To do so, system developers must better recognize and address the issues of reliability. The public has the right to require that systems are installed only after proper steps have been taken to assure reasonable levels of reliability.

The issues and questions concerning reliability that must be addressed include:

- 1. What risks and questions concerning reliability are involved when the computer system fails?
- 2. What is the reasonable and practical level of reliability to require of the system, and does the system meet this level?
- 3. What techniques were used to estimate and verify the level of reliability?
- 4. Were the estimators and verifiers independent of each other and of those with vested interests in the system?

In the intervening year, I am not aware that the developers of ANY computer system have made public their answers to these four questions. Readers of this forum will surely not leap to the conclusion that no computer system presents risks to the public worthy of discussion.

I would like to start a discussion on how we can change this. What can we do as professionals to make it the norm for system developers to present risk assessments to the public?

- * What can we do to make it more attractive to present a risk assessment?
- Explicitly invite developers of particular systems to publish draft assessments here in the RISKS Forum, with the promise of constructive feedback.
- Inaugurate a section in CACM for the publication of refined risk assessments of systems of great public interest or importance.
- Publish the risk assessments without refereeing. This gives the developers "first shot," gets the material out more quickly, and lowers the barrier to publication, without limiting the opportunity for public discussion and debate.
- Encourage developers to also address John McCarthy's question:
 - 5. What are the risks inherent in the best available alternative to the system in question?
- Encourage the exploration of legal steps that would make
 Risk Assessments as routine as Environmental Impact Statements.
 (This could be useful even if most of the former are as pro forma and unenlightening as most of the latter; they provide a starting point.)
- * What can we do to make it less attractive not to present a risk assessment?
- First, make it very clear that we, as a profession, believe that it is incumbent on system developers to present their risk assessments, and that delay or refusal amounts to malpractice of a very high order.
- Periodically publish (and publicize) the status of all outstanding invitations to present risk assessments.

- Bring cases of persistent noncompliance to the attention of ACM Council for appropriate action.

I present these suggestions as a springboard for discussion, not as a definitive program for action. I welcome suggestions for improvement.

Jim H.

Public Accountability

Peter G. Neumann <<u>Neumann@SRI-CSL.ARPA</u>> Thu 10 Oct 85 13:30:24-PDT

To: RISKS@SRI-CSL.ARPA cc: Horning@DECWRL.DEC.COM

Perhaps we can learn something from some steps that have been taken by the National Computer Security Center (although for security and not reliability). The NCSC (formerly the DoD CSC) has established a set of criteria for trusted computer systems, in the form of a range of increasingly stringent requirements. They have evaluated various systems against those criteria. They have also explored what kinds of applications should have which requirements. To date, two systems have been accorded high rankings: (1) the highest existing rating [A1] to the Honeywell SCOMP -- whose kernel design and trusted subsystems have undergone formal design proofs demonstrating that the kernel specifications satisfy a security condition of no adverse flow, and that the trusted subsystems satisfy other relevant properties involving privilege, integrity, and functional correctness; (2) a somewhat lower rating [B2] to Multics, which has not been subjected to any formal analysis, but which satisfies certain of the hardware and software-engineering criteria and which has withstood extensive penetration attacks. Other systems have also been evaluated, but given lesser ratings -- implying greater potential security risks. (The NCSC also publishes an Evaluated Products List.) The literature on this subject is extensive, but I note a few items here on the Criteria and on the SCOMP proofs. Other than that, you can look at the IEEE Proceedings for the Security and Privacy conferences each April and the National Computer Security Conferences held at NBS roughly once a year (previously called the DoD/NBS Computer Security Conference).

I of course need to add that the work on secure and trusted computing systems is only a very small part of that addressing the potential "risks to the public", which of course also involve reliability in various forms, human safety, timely responsiveness, etc. But my point is that some steps in the right direction are actually being taken in the security community -although those are still only small steps with respect to the overall problem. Nevertheless, something can be learned from the security work in addressing the ACM goals that Jim has reminded us of once again.

So, let us try to address some of Jim's points specifically in the future.
REFERENCES:

CRITERIA: Department of Defense Trusted Computer System Evaluation Criteria, CSC-STD-001-83. Write to Sheila Brand, National Computer Security Center, Ft Geo G Meade MD 20755. (SBrand@MIT-Multics)

SCOMP KERNEL DESIGN PROOFS: J.M. Silverman, Reflections on the Verification of the Security of an Operating System, Proceedings of the 9th ACM Symposium on Operating Systems Principles, October 1983, pp. 143-154.

SCOMP TRUSTED SUBSYSTEM DESIGN PROOFS: T.C.V. Benzel and D.A. Tavilla, Trusted Software Verification: A Case Study, Proceedings of the 1985 Symposium on Security and Privacy, IEEE Computer Society, Oakland CA, April 1985, pp. 14-31.

(Note: In a proof of design consistency, the proof must show that a formal specification satisfies a set of requirements, e.g., for security or fault tolerance. The difference between requirements and specifications in that case is generally that the former tend to be simply-stated global properties, while the latter tend to be detailed sets of constraints defined [e.g.,] functionally on state transitions or algebraically on inputs and outputs.)

Date: Tue, 8 Oct 85 16:26 EST From: Jan Lee <janlee%vpi.csnet@CSNET-RELAY.ARPA> To: RISKS@sri-csl.arpa Subject: The Titanic Effect

THE TITANIC EFFECT (Source unknown):

The severity with which a system fails is directly proportional to the intensity of the designer's belief that it cannot.

COROLLARY:

The quantity and quality of built-in redundancy is directly proportional to the degree of concern about failure.

JAN

Date: Wed, 9 Oct 85 09:43:20 EDT From: Brian_Borchers%RPI-MTS.Mailnet@MIT-MULTICS.ARPA To: risks@sri-csl.arpa Subject: Databases, Grades, etc.

Here at RPI, The Registrar's database, as well as the Bursar's systems are on the same machine that we use for academic work. We've put a lot of effort into making MTS secure... [By the way, some of this issue's discussions on the low risks of putting grades on student computers reflect overall a benevolent naivete about the system security risks. I have not tried to comment on each message individually, but find them intriguing. One could turn the students loose to see how many flaws they can find, perhaps as a part of a course: give them all F's in the database, and let them try to earn their A's by breaking in! On the other hand, you might find the last one who breaks changes some of the A's to F's! It is dangerous to announce in public that you as an administrator believe you have made unauthorized alterations difficult or impossible; knowing how badly flawed most of the systems are, that is a very large red flag to wave. But then you apparently need to be shown that you are wrong. Audit trails are great too, but watch out for the penetrated superuser interface. (This comment only touches the tip of the iceberg. Judging from this issue's contributions, I imagine the discussion might run for a while. Let's get down to specific cases if we can, but not just students' grades -- which are only an illustrative problem.) PGN]

🗡 Databases, Grades, etc.

<<u>Andy_Mondore%RPI-MTS.Mailnet@MIT-MULTICS.ARPA</u>> Wed, 9 Oct 85 11:36:54 EDT

Hal Murray in <u>RISKS-1.20</u> asks whether any schools are "brave/stupid enough" to have students and grades on the same computer. Well, that is the situation here. Administrators and students use the same mainframe. Administrative here generally use several extra layers of security such as extra passwords, allowing sign-ons to certain accounts only from specific terminals, and logging all successful and unsuccessful sign-ons to our accounts. So far, we in the Registrar's Office have not detected any unauthorized sign-ons (and we have never noticed any strange changes to files) although we occasionally detect an unsuccessful sign-on attempt from an unauthorized location. Generally, changing passwords frequently and using non-words and special characters for passwords seems to take care of the unauthorized access problem.

One thing that Hal did not mention is security problems when students and grades are on separate computers but on the same network, perhaps to share a special device or certain files. It seems to me that there could be almost as many potential security problems with this configuration as with my configuration. Does anyone have experience with this type of configuration and if so, what problems have you had?

🗡 Databases, Grades, etc.

Mark S. Day <<u>MDAY@MIT-XX.ARPA</u>> Wed 9 Oct 85 09:50:12-EDT

To: risks@SRI-CSL.ARPA

I tend to think that stories about crackers changing their grades should be taken with a fairly large dose of salt.

I once had the occasion to interview a vice-chancellor at my undergraduate university, and he explained the system there in some detail. Basically, they handled grades the way a bank handles money -- that is to say, there were 'audit trails' and paper copies of everything.

Discrepancies between what was in the computer and what was in the paper records would eventually get caught, even if there was a period of time when the wrong grades would show up on an official transcript. Correctly faking ALL the records so as to escape an audit would have required a great deal of knowledge (basically, it would have to be an inside job -- and they didn't have students working in these offices).

--Mark

Matabases, Grades, etc.

Peter G. Neumann <<u>Neumann@SRI-CSL.ARPA</u>> Wed 9 Oct 85 11:39:54-PDT

To: MDAY@MIT-XX.ARPA cc: Neumann@SRI-CSL.ARPA

Mark, I find myself disbelieving some of what you say. Manual comparisons tend to get done (if at all) when the data is entered. Auditing tends to get slighted, since people often tend to assume the computer is right! (The Santa Clara inmate who changed his release date did get caught, but perhaps only because a guard overheard him bragging about how he was going to get out early.) Most vice-chancellors (and many administrators) would probably tell you they are doing things right, and better than everyone else. That is the head-in-the-sand view of computing -- everything is just fine. But audit trails and paper copies of everything are not sufficient, even if they are diligently used. "Discrepancies ... would eventually get caught" is certainly hopeful, at best. Peter

Matabases, Grades, etc.

Mark S. Day <<u>MDAY@MIT-XX.ARPA</u>> Wed 9 Oct 85 14:51:40-EDT

To: Neumann@SRI-CSL.ARPA

Peter,

I still maintain that the scenario of "student changes grades to A's and lives happily ever after" seems dubious. It seems to be one of these apocryphal stories where everyone knows about someone who's done it, but there's little evidence floating around about it (sort of like stories about people putting cats in microwave ovens to dry them). Your other comments are well-taken. It certainly requires administrators, etc., to have a perception of the problem; that was one reason I was impressed by my interview with the vice-chancellor. Several years ago, crackers were not yet in the public eye, so I was pleasantly surprised to find out that anyone cared about the overall integrity of the grades database and talked about the need to regularly audit it.

--Mark

Matabases, Grades, etc.

Alan Wexelblat <<u>wex@mcc.ARPA</u>> Wed, 9 Oct 85 12:40:43 cdt

The University I attended had its database on a computer that student courses used. However, it was (is) a very well-kept secret. It is hard (under the OS of this system) to find out what people *might* log on. Also, it seems that hacker-types don't get the work-study jobs in the registrar's office. I'm not sure how long they can keep it up, but it's worked well for at least 5 years. (I only found out because I got to be good friends with the facilities people, and one of them happened to mention it.)

I guess this just reinforces the belief that human beings can make a risky or less-risky depending on how they use it. --Alan Wexelblat WEX@MCC.ARPA

Date: Wed, 09 Oct 85 16:12:15 EDT From: Ross McKenrick <CRMCK%BROWNVM.BITNET@WISCVM.ARPA> To: RISKS@SRI-CSL.ARPA Subject: Databases, Grades, etc.

Students and grades can exist on the same machine. Attempting to partition the students' and administrations' computing environments is a crude form of security which eliminates the possibility of providing students online services such as class lists and registration changes.

We take a two-fold approach to database security at Brown University: 1) prevention and 2) detection. We minimize our window of vulnerability by making it nearly impossible to gain unauthorized access to the programs which update grades, etc, and by making it nearly impossible to change a grade (even when authorized) without generating audit records, security log entries, and notifications slips for the professor.

We are not dealing with an EFT-type environment where "smash-and-grab" might work. A student is at Brown for four years, and his/her transcript is maintained by the Registrar forever. A student could theoretically change his/her grade for a day or two *in the computer database* (which does not mean that the grade, which is intangible, was actually changed). However, a system of checks and balances, built into and outside of the computer system, would eventually result in discovery, correction, and punishment. Suppose I could design a security system which was 90% (OK, 80%) secure. Then, rather than spend more time making it more secure (point of diminishing returns), I could spend my time on a recording/ reporting system which was 80% secure. Now, I finish by dovetailing the two systems to make it very unlikely that a hacker could survive both levels. Meanwhile, the Registrar, who is rightfully suspicious of computer security anyway, devises manual checks and balances which adds another level of security beyond the computer entirely.

Wouldn't it simply be easier for the hacker to forge a grade change slip from his/her professor? Now, considering all of this, you've got certain expulsion and prosecution under Rhode Island State Law hanging over your head.

Why would someone who's got all of this figured out have trouble passing courses, anyway?

A collegue of mine likens a malicious hacker in a fairly-well-secured computer environment to a bull in a china shop. The china is replaceable, the bull is dead meat.

Now comes the auto-theft-prevention-device philosophy: why pick on a fairly-well-secured environment when there are so many unsecured environments to fool with?

Security in computer-recordkeeping is a very serious subject. But you must keep it in perspective with the alternatives: manual record-keeping, locked doors and desks, etc.

Matabases, Grades, etc.

Randy Parker <<u>PARKER@MIT-REAGAN.ARPA</u>> Thu, 10 Oct 85 09:34 EDT

To: RISKS@SRI-CSL.ARPA

Regarding the subject of the risks of computer technology (in general) and large databases (FBI's NCIC, TRW, NSA, tenant/landlord database in California, and the Census), there is a reporter from the New York Times who has done quite a bit of research into it. His name is David Burnham, and his results a few years back are published in his book "The Rise of the Computer State" (paper/hardback).

The book is a call to arms to the millions who don't realize the serious threat to our freedom that this poses. Its shortcoming, as such, is that it is mostly a quite comprehensive series of anecdotal reports on various errors and abuses (incorrect warrants, Nixon abuse of phone company records, abuse by politicians, etc) of large informations stores. However, if you need convincing that this is a problem, you will find it in this book.

Burnham spoke here this past Tuesday and updated his list of "horror

stories", as he puts it. One number he gave, if my notes are right, is that an FBI audit of their NCIC showed that ~10% of the warrants proposed by this system are somehow based on incomplete or invalid information. He also mentioned proposals to increase the NCIC to include a White Collar Crime Index that would specifically contain the names of SUPPOSED white collar criminals and their ASSOCIATES. As Burnham pointed out, if they can't maintain the actual criminal information properly, what are the consequences when they start accumulating hearsay and gossip?

A serious problem is that no one has a real interest in keeping this information very correct, except for the falsely accused citizen, and, as Burnham pointed out, he doesn't have any way to correct it. I also agree quite heartily with Matt Bishop that "the greatest risk is not from the technological end but the human end." The technology itself is not to blame, but we need, especially as computer professionals whose opinions in the matter would be seriously regarded, to recognize the growing threat to our liberties and to act accordingly.

Randy Parker MIT AI Lab PARKER@MIT-REAGAN



Search RISKS using swish-e

Report problems with the web pages to the maintainer



<>

From: Friedrich von Henke (vonHenke@SRI-CSL)

I am temporarily acting as guest moderator of the Risks Forum. Peter Neumann had to go rather abruptly on an overseas trip, and the transition happened a bit disorderly. My apologies to all of you who were eagerly awaiting their twice-weekly cost of RISKS readings but had to go without. I hope to have things under control now.

Apparently the hiatus has had the effect of slowing down the stream of

contributions to a merely trickle; please don't hesitate to get the flow going again!

Friedrich von Henke

Date: 11 Oct 85 19:39:27 PDT (Fri) From: Nancy Leveson <nancy@UCI-ICSD.ARPA> To: RISKS@sri-csl.ARPA Subject: medical software incidents

I was just on a panel concerned with Software Safety at an IEEE conference on Computers in Medicine and heard about some more incidents involving software faults.

The first was cited in a recent RISKS forum message (about the programmable implanted pacemaker which was inadvertently reprogrammed by emitted magnetic fields from an anti-theft device in a retail store), but the patient was cited as having survived. Unfortunately, his weakened heart was unable to stand the increased pace, and he died.

Other recalls by the FDA involve:

1) An infusion-pump (used for insulin) had a software problem which caused the infusion of insulin or dextrose to be delivered at the maximum rather than the lower intended rate. This occurred when certain valid data was entered according to user instructions.

2) A programmable pacemaker "locked-up" when being reset by an external programming device. Luckily this occurred in a doctor's office, and the doctor was able to revive the patient.

3) A multiple-patient monitoring system was recalled because the software got patients' names mixed up with the wrong data.

4) An algorithm was incorrectly programmed in a diagnostic lab instrument which caused certain patient data to be reported erroneously as all zeros.

The reference for these incidents (for those who want to quote them) is: H. Bassen, J. Silberberg, F. Houston, W. Knight, C. Christman, and M. Greberman. "Computerized Medical Devices: Usage Trends, Problems, and Safety Technology," in Proc. 7th Annual Conference of IEEE Engineering in Medicine and Biology Society, Sept. 27-30, 1985, Chicago, Illinois, pp. 180-185.

Nancy Leveson University of Calif. Irvine

European activities

Udo Voges <<u>voges@LOCUS.UCLA.EDU</u>> Fri, 11 Oct 85 11:38:57 PDT

I would like to bring some activities to your attention which are going on in Europe, especially within and triggered by EWICS TC 7.

The European Workshop on Industrial Computer Systems (EWICS), TC on Systems Reliability, Safety and Security (TC 7) is working since about 10 years in this area, having some 100 members from industry, research and university. Previous work resulted in Position Papers on

Development of safety related software Hardware of safe computer systems Guidelines for verification and validation of safety related software Guidelines for documentation of safety related computer systems Techniques for verification and validation of safety related software System requirements specification for safety related systems

Current working areas include:

System integrity Software quality assurance and metrics Design for system safety Reliability and safety assessment

Besides conducting about four working meetings a year the TC is organizing the IFAC/IFIP Workshop on Achieving Safe Real-Time Computer Systems (Safecomp'79, '82, '83, '85, '86).

The results of the work of TC 7 are introduced into the standardisation process (IEC, ISO, and national bodies) as well as used by companies and licensing authorities.

Those interested in more information can either contact me or the current Chairman of TC 7: Mr. J.M.A. Rata, Electricite de France, 1 Avenue du General de Gaulle, F-92141 CLAMART FRANCE.

There exists an American counterpart to EWICS TC 7, but it was not possible to attract enough interested persons to keep it alive. The Japanese counterpart is also active, but due to the language barrier communication is minimal.

Udo

Robots are different

< <u>Saltzer@MIT-MULTICS.ARPA</u>> Sat, 12 Oct 85 01:30 EDT

To: risks@SRI-CSL.ARPA

When someone gets pinned to the wall by a robot, something different is going

on as compared to when someone gets gunned down by an FBI agent operating under incorrect information retrieved from the NCIC. Both cases may lead to specific tragedies, yet the example of risks from robots seems to me to be qualitatively different from many other computer-use risks.

The difference is that robots are used primarily in environments where mechanically-oriented people are accustomed to balancing the risks of new machinery against the benefits. These people have, over the years, learned to deal with risks from gear trains and drive belts, from swinging tailends on steamshovels, from runaway elevators, from inadequately supported cranes. They watch out, they learn from accidents, their insurers offer advice, they make mistakes and take risks, and they learn. To a first approximation, an industrial robot presents a risk similar in kind to other new machinery, and there is a moderately well-working system in place that is accustomed to watching for the risks. If anything, the average mechanic is suspicious of a new piece of machinery in direct proportion to its complexity, newfangledness, and gadgetry level, so is probably expecting the robot to screw up in marvelous ways. One might wish to argue with the particular balance that an industry has struck between risks and benefits, but it is unusual to find one in which mechanical risks are not understood at least moderately well.

The mechanic's suspicion of the new gadget is the essence of what seems to be missing in many other applications of computers, and why it is so important to raise awareness of the need to assess risks. I'm not convinced we need to harass our colleagues in the robot business with risk-consciousness-raising. We should be instead talking to their installers to find out what we can learn.

Jerry Saltzer

Automobile computer control systems susceptible to interference

Bennett Smith <<u>ircam!bks@seismo.CSS.GOV</u> > Wed, 23 Oct 85 11:14:29 -0100

By chance I saw an article in an issue of the "Journal of Environmental Engineers" (published in England, date of issue about 10 months ago, I believe) about the sensitivity of a microprocessor-controlled automobile control system to external electromagnetic radiation. As I recall, a CB transmitter near the car could, at the right frequency, make the engine slow down or speed up. Perhaps this article would interest some of your contributors.

Bennett Smith IRCAM 31, Rue Saint Merri 75004 Paris, France {seismo,philabs,decvax}!mcvax!ircam

Mathematics The human element

<>

15 Oct 1985 23:42:01 PDT

From: Dave Dyer <DDYER@USC-ISIB.ARPA> To: risks@SRI-CSL.ARPA

The human element really is where the action is, and it is a completely two-edged sword; Human actions which have the power to "fix" something almost inherently also give the power to "break" things equally severely. Conversely, weighty check and balance systems intended to prevent abuse end up preserving the status quo, however good or bad that may be.

The "police computer horror story" I'm most familiar with is illustrative. This is a well documented case I've been reading about in ACLU publications.

It seems some poor soul had his wallet stolen, and some criminal adopted his identity and later was involved in a robbery/murder. Through some circumstances peculiar to the case, the stolen identity, but not the culprit, were known to the LAPD. The detectives working on the case put the stolen identity into a national police computer. Our hero was stopped for a routine traffic citation, the computer coughed his name up, and he ended up on ice for a few days as a murder suspect.

So far, this is pretty harmless and understandable. Eventually the guy's identity and and non-involvement were establishd and he was turned loose. Then it happened again. And Again. The guy began carrying a letter from the local chief of police, saying he wasn't the guy the computer said was wanted, but that didn't cut it when he traveled.

The problem was that the LAPD detectives who put in the original "want" refused to remove it. Eventually the guy (and the ACLU) got the courts to mandate expunging the computer. I think the detectives involved and the LAPD are being sued. Quite rightly.

The point is, it is <<hard<> to design a system that can do its intended job, permit discovery and correction of errors, and resist unautherized or inappropriate use. I can't imagine a system that can do all three.

✓ Electronic Surveillance.

<> 24 Oct 1985 11:17-PDT

From: the tty of Geoffrey S. Goodfellow <Geoff@SRI-CSL.ARPA>

[forwarded to RISKS by Bill Keefe <keefe%milrat.DEC@decwrl.DEC.COM> from TELECOM Digest Volume 5, Issue 55, October 24, 1985]

Americans' Privacy Exposed by New Technology, Congress Told

By LEE BYRD - Associated Press Writer

WASHINGTON (AP) - The explosion in communications technology has so outpaced privacy laws that Americans have little or no protection against a plethora of new ways for government or private adversaries to pry into their lives, a congressional agency reported today.

The non-partisan Office of Technology Assessment found that 35 out of 142 domestic federal agencies use or plan to use various electronic surveillance methods, including modern devices not governed by a landmark 1968 law that circumscribed the use of wiretaps and bugs - concealed microphones.

The agency said 36 agencies, not counting those in foreign intelligence, already use a total of 85 computerized record systems for investigative or intelligence purposes, and maintain 288 million files on 114 million people. The report raised the "technically feasible" specter of these being linked into a single data base network that could track untold numbers of citizens without due cause.

The report, requested by House and Senate committees, noted that many new and uncontrolled methods of surveillance are made possible by the very technologies of which more and more Americans are availing themselves - electronic mail, computer conferencing, cellular and cordless telephones, beepers and electronic pagers. Intercepting such devices is easy, and "the law has not kept pace," the agency said.

But other devices, such as miniature television cameras and pen registers - which monitor the numbers called on a given telephone line - have enabled new ways to spy on people even if their own communications habits are more old-fashioned, the agency noted.

Rep. Robert W. Kastenmeier, D-Wis., chairman of the House Judiciary subcommittee on courts and civil liberties, said the study "shows how the law in this area has broken down; it is up to Congress to fix it. If we fail to act, the personal and business communications of Americans will not have the privacy protection they deserve."

Sen. Charles McC. Mathias, R-Md., said the report "documents how new and more intrusive forms of snooping have followed in the wake of the exciting advances in communications technology," and agreed Congress must "bring federal privacy laws up to date.'

Rep. Don Edwards, D-Calif., chairman of the House Judiciary subcommittee on civil and constitutional rights, said, "While the attorney general of the United States is claiming that the civil liberties granted by the Constitution should be limited to the 'original intentions' of the framers, the technological possibilities for government surveillance have exploded. The framers knew nothing of closed-circuit television, wiretapping and computer data banks."

The report noted that the Fourth Amendment, which protects "the right of the people to be secure in their persons, houses, papers and

effects, against unreasonable searches and seizures," was written "at a time when people conducted their affairs in a simple direct, and personalized fashion."

Neither, said the report, has Title III of the Crime Control and Safe Streets Act of 1968, which was designed to protect the privacy of wire and oral communications, kept pace.

"At the time Congress passed this act," the report said, "electronic surveillance was limited primarily to simple telephone taps and concealed microphones. Since then, the basic communications infrastructure in the United States has been in rapid technological change."

The congressional agency said it could not estimate the extent of electronic surveillance in the private sector, saying only "it is probable that many forms ... go undetected, and if detected, go unreported."

But in its survey of the federal bureaucracy, OTA found 35 agencies, mostly in the Justice, Treasury and Defense departments, used or planned to use:

-Closed circuit television, 29 agencies.

-Night vision systems, 22.

-Miniature transmitters, 21.

-Electronic beepers and sensors, 15.

-Telephone taps, recorders, and pen registers, 14.

-Computer usage monitoring, 6.

-Electronic mail monitoring, 6.

-Cellular radio interception, 5.

-Satellite interception, 4.

As for the 85 computerized record systems that could be used for surveillance purposes, none of the operators provided statistics requested by the OTA on record completeness and accuracy.

Under the 1968 law, wiretaps and bugs are prohibited without a court order based on the affirmation of a high-ranking prosecutor that a crime has occurred, that the target of the surveillance is involved, and that other means of investigation would be ineffective.

According to the Administrative Office of the U.S. Courts, federal and state judges approved 801 out of 802 requests last year for electronic surveillance, primarily wiretaps and hidden microphones, at an average cost of \$45,000.

The agency said that while there is some promise in emerging techniques for low-cost data encryption or other means to protect communication systems from eavesdropping, "there is no immediate technological answer ... against electronic surveillance."

Foreign intelligence cases are governed by a separate law, so the CIA, National Security Agency and Defense Intelligence Agency were not included in the survey.

Metwork Mailer Woes...

"UV2::MOOREL" <<u>moorel@uv2.decnet</u>> 0 0 00:00:00 CDT [sic! ed.]

To: "risks" <risks@sri-csl>

In a recent issue of one of the digests on the net, there was a problem mentioned that seems to have a bearing on risks on computer systems, particularly as use of computer networking increases in the future. At their request, the names have been changed to preserve anonymity.

Apparently for the past month, the people who reside on the bitnet have been unable to receive [this digest]. There is a long story behind this [...]. This story is also a *lot* of guesswork as to what happened.

At the beginning of September, [our system] changed its host name to conform to the new domain name standards. The site we were using to get to bitnet, did not recognize the new name and began rejecting all mail from [our system]. We did not become aware of this because we were not receiving any rejections or errors back from the gateway. We were however, receiving mail *from* the people on Bitnet who were asking what happened to their [...] digest.

We attempted to contact the people at [the gateway] but of course the mail failed and they never did anything to correct the problem which they, of course, were not aware of because nobody was complaining. (Sounds like a Catch-22 situation if I ever heard one).

In any case, the problem has now been resolved. Unfortunately, these people have missed close to 50 digests. There is no way I can tie up the mailer at [either the host or the gateway] in order to remail the messages. I also understand that there is no way to use FTP from the bitnet.

It appears that several incidents conspired together to cause the loss of this information, and although the loss was not critical, it will take much time and effort for the people involved to catch up. If this had been a more critical information transfer, it might have been corrected faster; however, there is a good chance that it would have gone undetected anyway. It seems to be one more reason for information about any potential changes to be passed on to any sites that may be affected and to be thoroughly checked on both ends to prevent this kind of thing from reoccurring.

Lynne C. Moore (Moorel@Eglin-Vax.Arpa)

✓ Grade changing.

<<u>Karl.Kluge@G.CS.CMU.EDU</u>>

Some doubt has been expressed in this forum recently about people changing grades and living happily ever after. I can't talk about college systems, but in high school all the grades, attendence, etc. for my high school and several other high schools were kept on a mainframe in a centralized location. There is a system in Michigan called MOIS for vocational data, and on the back of my MOIScript on computer science was the transcript of a terminal session between the attendance people and the computer. The login message gave the phone number of the mainframe. The password was overprinted, but that is useless -- you can learn to read through almost any overprinting. Access to the grading, course scheduling, and attendance programs was by providing a social security number which was echoed and not overprinted. I thus found myself able to do really miraculous things. Being sixth in my high-school class, I had no real motivation to use my knowledge maliciously, and informed the administration. Some safeguards were added (old social security numbers retired, certain social security numbers only giving access to certain programs, restricting access to certain programs to certain accounts), but I'm sure those could have been circumvented with minimal effort -- I was a fairly good systems hack on the operating system, and there were people who could hack rings around me. The operating system was a simple three-tier ring system, and a lot of the features put in for the sake of usability made it very insecure.

I send this to give first-hand evidence to those who have been posting doubts that such things happen.

🗡 Databases, grades, etc.

<<u>Andy_Mondore%RPI-MTS.Mailnet@MIT-MULTICS.ARPA</u>> Wed, 16 Oct 85 17:11:36 EDT

One of the systems programmers here at RPI made a point about administrators and students sharing the same computer: You really aren't that much more secure when you have administrators and students on separate computers if there is a network or dial-up connection to the administrative computer than you are when administrators and students are on the same computer. If you have network or dial-up connections to an administrative computer, it isn't too difficult for a student with an autodial modem to write a program on a PC that simply tries all possible phone numbers for certain telephone exchanges and record the numbers that produce a carrier tone. Then the student could have another program that tries passwords unless the system disconnects the line after a certain number of unsuccessful tries. The major advantage of separating administrators and students is that it might be more difficult for a student to access an administrative file from a student account assuming the administrative file has the proper protection set.

🗡 Database, Grades, etc...

< <u>Sienkiew@louie.udel.EDU</u>> Mon, 21 Oct 85 0:44:24 EDT

You can create an extremely effective audit trail if you think about it for a while. That just makes the problem more "challenging".

Suppose you do your auditing one day and find that there were unauthorized grade changes made for every student in the CS department and 1/2 of them requested (incorrect) printed transcripts. It seems unlikely that everybody

independently broke in on the same day. So who do you penalize? How many transcripts have been mailed out already?

Suppose no grades were changed but there is a trojan horse waiting to raise the grade only under certain circumstances?

My point is that the data doesn't have to stay changed forever. And you can't check the auditing records for every transaction, if you expect to gain by using the computer. You need to do as much as you can, of course, but beware of the false sense of security...

Mark.



Search RISKS using swish-e

Report problems with the web pages to the maintainer



Peter G. Neumann <<u>Neumann@SRI-CSL.ARPA</u>> Mon 18 Nov 85 12:57:03-PST

To: RISKS@SRI-CSL.ARPA

We have been talking about risks to the public in the use of computer systems in this forum since 1 August, and trying to keep the discussions mostly technical -- but not political or polemical. On the other hand, I have noted on various occasions that it is sometimes hard to exclude nontechnical arguments. This message may initially seem off the mark, but I think it has some subliminal relevance that might help put into perspective the importance of the underlying assumptions that we make and the need to anticipate essentially all possible unusual circumstances.

On 13 October 1985, in Florence, Italy, at about 10:05 PM, European Standard Time, my apparently very healthy 19-year-old son Chris -- never having had a medical problem in his life -- suddenly had his heart stop and died within moments. Resuscitation attempts failed. The autopsy found no discernible apparent cause of death. A neurophysiologist friend who joined me in Florence suggested ventricular fibrillation as the most likely actual cause. The heart muscles receive signals from distributed sources via independent paths, and normally all of the signals arrive sufficiently synchronously to trigger heart contraction. Under fibrillation, the signals arrive incoherently, and cannot be integrated sufficiently to trigger contraction. So, why do I mention this in a RISKS Forum? Well, even in an apparently completely healthy person there exists some risk of spontaneous malfunction. It seems to me that in making arguments about how hardware and software will operate correctly or will continue to operate correctly if they once did, we make all sorts of implicit underlying assumptions that may be true most of the time, but that may indeed break down -- particularly in times of stress. The nastiest problems of all seem to involve unanticipated conditions in timing and sequencing, in both synchronous and ansynchronous systems, and particularly in distributed systems. We have seen various problems in the past -- the ARPANET collapse (due to an accidentally propagated virus, after years of successful operation) and the first shuttle launch immediately come to mind as specific well-documented examples. In some cases there is also signal inference -- as in the pacemaker problems (see Nancy Leveson's message in **RISKS-1.22**). I think that in our lives as in computer systems, we tend to make unjustified or oversimplified assumptions. In life, this makes it possible for us to go on living without inordinate worrying. However, in computer systems, greater concern is often warranted. So, my point in introducing this message into the RISKS Forum is to urge us to try to make our assumptions both more explicit and more realistic. Basing a system design on assumptions that are almost but not quite always true may seem like a close approximation, but may imply the presence of enormous unanticipated risks. In systems such as those involved in Strategic Defense, for example, every one of the potentially critical assumptions must be sufficiently correct.

Peter G. Neumann (back again on the net)

Safety Group Activities in the U.S.

Nancy Leveson <<u>nancy@ICSD.UCI.EDU</u>> 09 Nov 85 13:04:51 PST (Sat)

Udo wrote about the EWICS TC7 in a previous RISKS forum and said that such a group died through lack of interest in the U.S. Actually, there is a similar group which has been active in the U.S. for about three years. It is called the Software System Safety Working Group and was started by the Air Force although it is now a tri-service group. Although sponsored by the DoD, it is not limited to military applications and has participants from other branches of the government and industry. The latest meeting was held in conjunction with a conference on computers in medicine.

Meetings are held approximately twice a year and usually have from 50-200 participants. One of the products of the group is a Software Safety Handbook which is meant to accompany the recent MIL-STD-882b (System Safety) update. The main purpose of the group has been to meet and discuss new techniques, share experiences, exchange ideas, etc. There is tentatively a meeting planned for January in Washington D.C. Anybody interested in the group should contact me (nancy@uci.edu) or Al Friend (friend@nrl-css) who is with the Navy and is currently chairing the group. A future plan is to have an on-line

safety database which will reside at the SRI NIC.

Other activities in which I have been asked to participate and which might be of interest to readers of this forum are a conference on safety which will be held in Washington D.C. next July and a workshop on safety and security sponsored by the Center for Software Reliability in England next September. I am also considering organizing a workshop in California on safety which would be held right before the next International Conference on Software Engineering in Spring 1987. Anyone interested in more information on any of these activities can again contact me and I will direct you to the right people.

Nancy Leveson University of California, Irvine

***** Automobile computer control systems susceptible to interference

Bennett Smith <<u>ircam!bks@seismo.CSS.GOV</u> > Wed, 23 Oct 85 11:14:29 -0100

By chance I saw an article in an issue of the "Journal of Environmental Engineers" (published in England, date of issue about 10 months ago, I believe) about the sensitivity of a microprocessor-controlled automobile control system to external electromagnetic radiation. As I recall, a CB transmitter near the car could, at the right frequency, make the engine slow down or speed up. Perhaps this article would interest some of your contributors.

Bennett Smith IRCAM 31, Rue Saint Merri 75004 Paris, France {seismo,philabs,decvax}!mcvax!ircam

// Irresponsible computer "game"

Ted Shapin <<u>BEC.SHAPIN@USC-ECL.ARPA</u>> Mon 18 Nov 85 11:54:52-PST

To: risks@SRI-CSL.ARPA, human-nets@RED.RUTGERS.EDU Phone: (714)961-3393; Mail:Beckman Instruments, Inc. Mail-addr: 2500 Harbor Blvd., X-11, Fullerton CA 92634

From a Toys R Us ad in the L.A. Times, 11/17/85:

Activision HACKER Makes you feel like you've unlocked someone else's computer system! For C-64, C-128. \$24.97.

[And on the package:]

TEMPTATION

HACKER

To stumble into somebody else's computer system. To be someplace you're really not supposed to be. And to get the strange feeling that it really does matter. "LOGON PLEASE" is all you get to start with. That's it. From there, it's up to you. If you're clever enough and smart enough, you could discover a world you've never before experienced on your computer. Very tempting.

This "product" is socially irresponsible! It leads young people to think breaking into unknown systems is OK. The "world" they discover may be the world of the penal system!

Ted Shapin

BBS Legislation

Ted Shapin <<u>BEC.SHAPIN@USC-ECL.ARPA</u>> Thu 14 Nov 85 10:34:50-PST

To: human-nets@RED.RUTGERS.EDU, risks@SRI-CSL.ARPA

I have remailed several messages on pending BBS legislation to INFO-LAW@sri-CSL. One is a draft of a bill by Senator Leahy's aid Podesta which is a good bill. People interested in preserving open communcation via BBS's may wish to read these items. Ted Shapin.

Arms-Discussion Digest V5 #8 [EXCERPT: SDI Debate]

Moderator <<u>ARMS-D-Request%MIT-MC.ARPA@MIT-XX.ARPA</u>> 29 Oct 85 09:33-EST

To: ARMS-D%MIT-MC.ARPA@MIT-XX.ARPA Reply-To: ARMS-D%MIT-MC.ARPA@MIT-XX.ARPA

EXCERPTED FROM Arms-Discussion Digest Tuesday, October 29, 1985 9:33AM Volume 5, Issue 8

[There is sufficient NONOVERLAP in our readerships to warrant reproducing this. Apologies to those who have read it already. PGN]

Date: Mon, 28 Oct 85 10:58 EST From: Mills@CISL-SERVICE-MULTICS.ARPA Subject: SDI Debate

This is a summary of my impressions of the panel discussion/debate entitile "Star Wars: Can the Computing Requirements be Met?" This took place on Monday October 21 at MIT. The panelists where Danny Cohen, David L Parnas, Charles L Seitz, and Joseph Weizenbaum. The moderator was Michael L Dertouzos. I was basically disappointed in this panel discussion. I was hoping to hear a good counter to the the arguments Dr Parnas had put forth in his papers. Dr Cohen started what looked like an organized attack on Dr Parnas' "Octet", refering to the series of eight papers Dr Parnas presented his arguments in. Dr Cohen correctly dismissed the eighth paper,"Is SDIO An Efficient Way To Fund Worthwhile Research", as being outside the bounds of the current discussion. Unfortunately Dr Cohen only further discussed one of the other papers. The other six where dealt with with some minor hand waving. I have to admit I don't remember which paper Dr Cohen "went into detail" on. This is because the detail amounted to a one slide outline of the major six points of this paper. This slide was up for no more than one minute with some more hand waving that none of these points were true.

Back to the side claiming the software is not feasable, Dr Weizenbaum didn't realy add much of anything to Dr Parnas' arguments. He thought that Dr Parnas had done a wonderful job and there wasn't much he could add. He gracefully didn't take up much time saying this either. Dr Parnas basically presented the material in his papers. He added the new point that even if we build this thing and it "tested OK", we could never realy trust it and would be forced not to rely on it.

Charles Seitz made no attempt to directly attack Dr Parnas' argument. He focused his presentation on a simplistic hierarchal structure the software for SDI could take. Unfortuanately this looked like a highly centralized form of controlling all the weapons and sensors resulting in a high degree of complexity and size.

Both Dr Cohen and Seitz hit upon the point that the software for SDI is not necessarily as large and complex as some people might think. They claimed that it could be built of smaller fairly independant parts. To me this appeared contradictory to Dr Seitz's hierarchal control structure. It did come through that If you had enough totally independant platforms shotting things down, you stood a good change of hitting most the targets. It is also clear that you would need a very high level of overkill to make this work since the other platforms don't know who else is shotting at what.

Back to Dr Parnas' points, I did get the feeling that there is some general agreement that there is a limit to the scale and complexity our software engineering can handle. Dr Parnas furthered this point by saying large advances in the mathematics of discreet functions are going to be a major stumbling block in the furthering software engineering. He doesn't expect these large advances on the grounds that if you simplify the equations to much you are loosing information. A discreet function can only represent so many bits. I may not have this argument exactly right. He also went thru his standing arguments against AI or automatic programing helping very much.

[I think the argument is that we need concise, manipulable discrete functions modelling software in order to achieve what other fields of engineering can do with concise, manipulable

continuous functions. However, such concise representations may not be possible due to information-theoretic constraints on the number of bits that can be represented by a certain number of symbols. --MDAY@MIT-XX]

[I didn't get quite this impression, though I agree with it. Rather, I thought Parnas was saying that the problem was in the fact that with software that is fundamentally digital, there is no such thing as a continuous function, and that therefore the usual engineering assumption valid in most of the world that small changes in input or in correctness necessarily mean small changes in output or result simply isn't valid in the software engineering world. Until it is possible to analyze software in terms of approximately correct functions, graceful software degradation (in terms of an approximately correct program always doing approximately correct things) is not really possible. -- LIN@MIT-MC]

Both sides came up with a number of interesting and colorful analogies. The most relavent is the Space Shuttle. Dr Cohen claims that the Space Shuttle works. This is obviously true in some sense. However, it was also pointed out that there have been times when the software on the shuttle has not worked within seconds of launch. It seems that it would be impractical to ask the Soviets to wait 15 minutes while we reboot the system.

[Indeed, Seitz conceded that under certain circumstances plausible in the context of a nuclear missile attack, it might be necessary to re-boot the system. He then proceed to ignore the consequences of that; he did not even say that there are ways to eliminate the need for re-booting. -- LIN@MIT-MC]

In summary it seems that there are very real limits on what our software engineering can handle reliably. We are actually not that far from those limits in some of our current efforts. If SDI is to work its architecture must be dictated by what is doable by the software. It is unclear that SDI is feasably from a material cost point of view if the platforms are small and independant enough to be reliable from the software standpoint.

In closing I would like to say that I don't think either side did a particularly good job sticking to just the software feasibility issue. One other interesting thing happened. Dr Parnas claimed to have asked some person with authority over SDIO whether "No, we can't do this" was an acceptable answer. He did this for the first time at this debate because he did not want to say this behind this person's back. Unfortunately, I don't remember this other person's name, but he was in the audience. Dr Parnas claims that the answer was, "No is not an accepatble answer" and challenged the other person to deny this. The other person promptly stood up and did exactly that.

[If you mean that it was political, that's certainly true. But politics is really the determinant of the software specifications at the top level. That is how it should be, and people who want to ignore that are ignoring the most important part of the problem.
However, in other instances, the Administration has noted that the SDI is central to future US defense policy. In addition, it has never specified what evidence it would consider adequate or sufficient to turn off the SDI.
-- LIN@MIT-MC]
✓ Image: Constraint of the problem is constraint of the maintainer.
Search RISKS using swish-e.
Report problems with the web pages to the maintainer.



Often the discussion has touched on failure of software and hardware, but rarely on levels and methods of protection that should be built into these systems. Is is good to trade cycles for protection? What are the best ways to recover from failures? Does anyone have real experiance with these questions?

Brad Davis

[Clearly these are leading questions! We have indeed mentioned many good techniques of software engineering that help. But there are no easy answers -- especially in the absence of specific requirements. But let's see if any of our readers wants to take a crack at this one. PGN]

*X*Space Program Software

Jerome Rosenberg <jerome@rsch.wisc.edu> Tue, 19 Nov 85 14:46:49 CST

We have heard a great deal about the great successes of the space program but we rarely hear about the difficulties that have to be overcome with great effort and dedication. I suggest you direct your readers to the current issue of DATAMATION for an article by Edward Joyce entitled "The Art of Space Software". Its subtitle tells a far different story than some hand-waving protagonists of the SDI tell about the Space software. The subtitle -- The complicated software labyrinth behind the shuttle is still far from error-free -- tells the story. The article should serve to alarm those who are quick to discount the sincere critics of the SDI software problems. jerome @rsch.wisc.edu

Tuesday, 19 Nov 1985 10:21:51-PST brewer%ace.DEC@decwrl.DEC.COM (too busy for bureaucracy -John 5522026)

Subject: Re: Susceptibility to interference

RE: Bennett Smith's comments of emi-rfi susceptibility in automobile control applications... cb's are low power, limited frequency devices. As an Amateur radio operator, one has to be aware of much higher output power, as well as a much wider bandwidths. Amateur Radio frequency allocations include segments from 1.8Mhz to Ghz ranges.

As I remember, some of the control modules are also pretty good emitters of Emi/Rfi hash as well. Typical (legal) output power of a CB is 5 watts or less. A typical ham radio mobile transmitter output power is 100-200 watts.

Something to think about! -John

Tue, 19 Nov 85 15:10:41 EST From: Herb Lin Subject: Expecting the unexpected

Regarding your comments about spontaneous failure: The Russians have a saying regarding rifles used on stage in plays: once every decade an unloaded gun will fire; once every century a rake will fire.

[Perhaps that is what prompted Stravinsky to stage "The Rake's Progress". PGN]

Wednesday, 2 Oct 1985 21:32:34-PDT From: kaiser%furilo.DEC@decwrl.ARPA (Pete Kaiser, 225-5441, HLO2-1/N10) Subject: Philip W. Anderson's "Case Against Star Wars"

[The following message was put aside for evaluation before my absence. With the reminder that we of course would like to see more informed pro-SDI contributions in RISKS as well, Anderson's article seems worth including -- not because it breaks new ground, but because it represents a position for discussion. PGN]

The article below, by Professor Philip W. Anderson of Princeton University, appeared in the Princeton Alumni Weekly of September 25, 1985, and is reprinted here with the author's permission. Professor Anderson won the Nobel Prize for Physics in 1977, and was awarded the National Medal of Science in 1982.

Although what Professor Anderson has to say is couched partly in specific terms of Princeton University and the discipline of academic physics, it seems to me relevant to basic research in general, and to computer science research and the discipline of computer science in particular. To me, for instance, it seems to be very personally a social consequence of the military funding of computer science research that, while I've worked with computers, there have been many kinds of work which I couldn't conscientiously do because, although they may be very interesting, they are done essentially only for military purposes and with military funding.

Finally, Professor Anderson points out that a great deal of sensible thought can be brought to social issues even by someone who "isn't ... fascinated by the technical details." Agreed. We must remember that we're not priests.

---Pete

Kaiser%BELKER.DEC@decwrl.arpa {allegra|decvax|ihnp4|ucbvax}!decwrl!dec-rhea!dec-belker!kaiser DEC, 77 Reed Road (HLO2-1/N10), Hudson MA 01749 617-568-5441

> The Case Against Star Wars Philip W. Anderson, Princeton

I am not an expert on strategic weapons. I'm a theoretical physicist who has been involved in almost all of physics except atomic bombs. I have not done classified work since 1945, and that was on radar. My total contribution to the laser -- a major technical component of the Strategic Defense Initiative, which is better known as Star Wars -- was roughly that when one of the scientists at Bell Laboratories who originated the things asked me to predict whether a certain seminal version of it would work if they built it, I said "Well, maybe."

Fortunately, most of the scientific issues that come up in discussing Star Wars are very simple ones which require neither specialized nor especially technical -- and therefore classifiable -- knowledge. One needs to know that it costs everyone about the same amount to put a ton of stuff into a given orbit and that this is a major portion of the cost of any space system; that signals can't travel faster than the speed of light; that it takes roughly as much chemical fuel to burn through a shield with a laser as the shield itself weighs; that Americans are not measurably smarter than Russians; and a few other simple, home truths. Given these, almost everyone comes to much the same conclusions.

If you go through the enormously detailed kinds of calculations on specific configurations which Richard Garwin and his fellow opponents of SDI felt necessary to convince the stubborn, you leave yourself open to the kind of errors of factors of 2 or 4 which Martin Muendel '86 found in his widely publicized junior paper last spring [Princeton Alumni Weekly, May 8] and which then -- to the lay person -- seem to weaken the whole structure. This is a particularly tough game because Star Wars advocates do not themselves propose specific configurations and present specific calculations that can be shot down; their arguments are given in terms of emotional hopes and glossy presentations. This is why I think it is good for the argument against SDI to be made by a mentally lazy, non-expert person like myself who isn't particularly fascinated by the technical details.

The reasons for not building Star Wars are essentially identical to those which led both us and the Russians to abandon, for practical purposes, the antiballistic missile in 1972 and to sign a treaty restricting ABMs. It is important to understand that reasoning -- and perhaps it is less emotionally charged than Star Wars since it is now history and not even controversial history anymore. Why would anyone feel that a defense against missiles was useless and, in fact, dangerous and destabilizing?

There are three stages, each more certain than the last: (1) It probably wouldn't work, even under ideal conditions. (2) It almost certainly wouldn't work under war conditions. This puts us in the dangerous and unstable situation of the gunfighter who doesn't know if his gun is loaded. (3) Most certain and conclusive of all, *each defensive system costs, inescapably, at least 10 times more than the offensive system it is supposed to shoot down*. Thus it pays the other side to increase its offensive arsenal until the defender is bankrupt, and the net result is an *increase* in armaments and a far more dangerous situation, without any increase in safety.

The offense has, inescapably, enormous advantages: its missiles are sent at will, in any desired sequence and quantity, with any number of decoys and other deceptive countermeasures, preprogrammed at leisure to hit their targets; the defense has to find them, sort them out, get into space at a time not of its own choosing, and then kill the warheads it finds with nearly perfect accuracy. In the case of ABM, there were other problems, such as that the explosions were over the defending side and that the first few explosions probably blacked out the whole shooting match, but that was sufficient argument against.

As far as almost everyone in and out of the Defense Department was concerned, until March 1983 this situation was an accepted fact. No technical breakthrough had or has changed those realities. The change has been purely political and emotional, and hence now financial. President Reagan's March 1983 speech, as far as anyone can ascertain, was not preceded by any serious technical review, but quite the opposite: the most recent and urgent internal study of antimissile defenses had come out negative on all possible schemes.

Apparently, the President based his speech and his subsequent program on a collection of rather farfetched suggestions -- farfetched but by no means secret and previously unknown -- which, to the outside scientific observer, seem to

deserve the oblivion that the last pre-Star Wars study consigned them to. These schemes amount to a way for the defense to spend more per missile and still let through a large fraction of the offensive missiles. The defensive hardware that has to be got up into space still has to have roughly the same mass as the offense; in many schemes it has to get there faster; and it still has to be much more sophisticated and therefore vulnerable and delicate. Key components, in most schemes, have to be left in space indefinitely, inviting the enemy to track them with space mines, perhaps the most dangerous tripwire mechanism for stating a war that one can possibly imagine.

Some Star Wars advocates will protest that I do not mention the one idea which doesn't founder just on the problem of total mass in space. This is the scheme of exploding hydrogen bombs in space and directing the explosive energy of the bombs with lasers to kill very many missiles per bomb -- several hundred to several thousand, if one is to kill an equivalent cost in missiles! If I could think of any way such a monstrosity could work as opposed to the many ways it could not work or be frustrated, I would take it more seriously. Apparently there has been some good and interesting science done on these lasers, but unfortunately it is classified; no one, however, seems to claim that it helps much with the technical problem. I cannot, incidentally, see any way to do meaningful development on such a weapon without exploding H-bombs in space, a terrible pollution as well as a violation of what treaties we have.

I think the above would represent reasonably well the views on the technical realities of most trustworthy physicists to whom I have spoken, in or out of academia and in or out of the Star Wars program. In academic physics departments, which receive relatively little support from the DOD, a pledge form has been circulating stating that the signer opposes SDI as unworkable and will not seek SDI funds; this has had a high percentage of signers everywhere it has been circulated and its preliminary circulation in Princeton over the summer encountered only a few holdouts. Those who do not sign feel, primarily, that research in any guise shouldn't be opposed, while agreeing personally that the systems proposed are unworkable and destabilizing.

Perhaps it would be worthwhile, therefore, for me to explain why I feel the large increment of research funds earmarked by President Reagan for SDI is a very bad thing for the research community, as well as for the country as a whole. You will note that I said *increment*; every year before Star Wars, we spent \$1 billion in ABM research and development. My main reason is that, on the whole, Star Wars will represent a further acceleration of three extremely disturbing trends in the direction of research funding in this country.

First, we are seeing a decrease in basic research relative to mission-oriented, applied research. The basic research agencies -- National Science Foundation, Basic Energy Sciences in the DOE, and National Institutes of Health -- have been maintained at level funding while their missions have been gently skewed toward applications and engineering by piling more applied responsibilities on them. At the same time, while the Administration has cut back on development in some civilian sectors, it has more than compensated by increasing the amount of applied work for the military.

Second, there is a trend away from scientific administration of federal research money -- mostly done by the system of "peer review" -- to micromanagement either

by bureaucrats, or, increasingly, by Congress, with all the logrolling possibilities that entails. The three institutions mentioned above, especially NSF and NIH, operate by subjecting each grant to a jury or other scientists. Like most democratic procedures, this system is worse than everything except the alternatives; its effect has been reviewed repeatedly and there is no serious doubt that it works. Military "research," on the other hand, has always operated on the arbitrary whim of the contracting officers. In the early days after World War II this administration was a benevolent despotism, but the adjective has long since lost its meaning. Most of the in-house DOD laboratories have been rather a scandal in the research community. The dominant motivation in this system seems to be the standard bureaucratic one of "empire building."

Third, from the point of view of the country as a whole, perhaps the most dangerous trend is the shift from civilian to military dominance of our federal research and development spending. Under the Reagan Administration, this has grown to 72 percent military, up from about 50 percent a decade ago. Everyone has been told -- and DOD sees to that -- of the great economic benefits of "spin-off" from military development, but if they exist (and I have never found an economist who believes in them), they are not evident in our recent economic performance vis-a-vis Japan and Germany. In fact, in a country like ours with a serious shortage of trained engineers and scientists, a shortage which would be crippling if we did not attract great numbers of them from overseas to staff our universities and research laboratories, the waste of our precious technical expertise on military hardware is a serious economic debit.

From Princeton's point of view, all of these trends are disturbing. As a topflight research university, a heavy percentage of our funding is in individual support of independently functioning basic scientists, mainly peer-reviewed and to a large extent from the agencies mentioned above. We have not had to resort to logrolling political tactics, nor have we had to accept micromanagement, DOD control of publications, or limitations on citizenship of students to keep our research funded. SDI control of funding, and in general the shift of research funding to the military, is a serious danger to the independence of Princeton as a research university.

Of course, this is a narrow and slightly parochial view, but it is nonetheless serious. Certainly it is more important that the naive emotional appeal of the Star Wars concept is being used so blatantly to defuse the country's strong desire for nuclear disarmament, and to turn this emotional pressure into yet another excuse for enriching the arms manufacturers and building up a dangerous and worthless arsenal of nonsensical armaments. To paraphrase Murph Goldberger's testimony on the ABM: Star Wars is "spherically" senseless -- that is, silly no matter how you look at it.

[End of Philip Anderson's statement, and of Pete Kaiser's Message.]

 Image: Arrow of the state of the state



Peter G. Neumann <<u>Neumann@SRI-CSL.ARPA</u>> Sun 1 Dec 85 16:00:32-PST

This is a short note on the subject of how little we understand or are willing to admit about long-term effects (whether eventually very obvious effects or sometimes long-hidden side-effects) -- and of how, even if a risk is known, it may be suppressed.

The front page of today's NY Times (Sunday 1 Dec 85) has two articles on Bhopal, one year after. Stuart Diamond's article begins, "Medical studies conducted in the year since the chemical leak ... indicate that the chemical responsible for the accident causes serious long-term health problems that were unknown before the disaster." Furthermore, the Bhopal problems appear to have been due not just to the pesticide ingredient methyl isocynate, but to an unforeseen chemical reaction that transformed so



Search RISKS using swish-e

Report problems with the web pages to the maintainer



Matt Bishop <<u>mab@riacs.ARPA</u>> 2 Dec 1985 0926-PST (Monday)

In <u>Risks 1.25</u>, you wrote a very good article pleading for greater humility. I'd like to add a little to that. Very often a solution is proposed which alleviates the symptom, but aggravates the cause, of the problem. (Draw your own examples, folks -- the best ones are political, and I'm not touching THOSE with a ten-foot pole!) Unfortunately, those are often the most appealing because they let us forget, for a time, that the problem exists. When it returns, the symptoms are different but the root cause is still there -- and more rotten than ever.

As another thought, I've found that in order to ask the question that leads to a solution for a problem you have to know most of the answer already -- it's merely a matter of synthesizing the various parts into a whole. (As an example, Riemannian geometry existed before Einstein put it to use; it was a mathematical toy, done to prove the Fifth Postulate was just that, a postulate.) But for all non-technical problems, science alone cannot provide the answers -- it can provide techniques for solving the technical components, but no more. And when people forget this, disaster follows, because science is used to treat the result, rather than the cause. (Incidentally, "science" is not the culprit. The same thing happens in spheres where science takes a back seat to ethics and morality -- and what I said still applies. No one discipline can provide a complete answer to any non-technical problem. Unfortunately, an incomplete, but complete-looking, answer can usually be obtained from any discipline -- and this is what we must avoid doing!)

Matt

// Reliable Computer Systems

Jim Horning <<u>horning@decwrl.DEC.COM</u>> 2 Dec 1985 1354-PST (Monday)

Although reliability is only part of risk assessment, it is an important one. I would like to bring to the attention of this forum a book to which I made a modest contribution.

"Reliable Computer Systems: Collected Papers of the Newcastle Reliability Project," edited by Santosh K. Shrivastava, Springer-Verlag, 1985, xii + 580 pages, ISBN 0-387-15256-3 (New York) and 3-540-15256-3 (Berlin).

This volume brings together in one place more than 30 papers by more than 20 authors reporting more than a decade of research on reliability. It contains papers that survey the issues, define terminology, propose partial solutions, and assess the state of the art.

<



Search RISKS using swish-e

Report problems with the web pages to the maintainer



would take me longer than I have to try to edit it. PGN]

From nzm10 Thu Dec 5 15:26:10 1985 Relay-Version: version B 2.10.2 9/18/84; site amdahl.UUCP Posting-Version: version B 2.10.2 9/18/84; site amdahl.UUCP Path: amdahl!nzm10 From: nzm10@amdahl.UUCP (Neal Macklin) Newsgroups: amdahl.general Subject: worms and viruses (long) Date: 5 Dec 85 23:26:10 GMT Date-Received: 5 Dec 85 23:26:10 GMT Distribution: amdahl Organization: Amdahl Corp, Sunnyvale CA

This came off the VM conf system, and I thought it was interesting.

The first part is posted outside my office, so those of you that have read that should go to line 530 (approx).

(I hate people who say "enjoy".....Neal)

* TOPIC: RUMOR - "RUMOR Interesting tidbits about the company" --> Item 15 from AJP30 on 12/02/85 at 16:22:58

This is part one of a two part series written by Gary North about software worms and viruses. Gary North is an investment newsletter publisher and presents an interesting perspective of the problem from a non-technical point of view. Enjoy.

Andrew J. Piziali, x8584.

Gary North's Remnant Review Matt. 6:33-34

Vol. 12, No. 20 379

November 1, 1985

What you are about to read will shock you. It shocked me as I did the research on the project. It so completely shocked me that I am lifting the copyright on this issue and the one to follow. Reprint them in any form you choose.

Second, I am sufficently scared about what I've uncovered that I am going to make this request. I will pay \$1,000 to the first person who blows what I regard as significant holes in my thesis, and who consents to a 90-minute taped interview for FIRESTORM CHATS. If you can't do this, but you can put me in contact wth anyone who can refute me or show an effective way out of the problems I raise, I WILL GIVE YOU A ONE YEAR RENEWAL TO REMNANT REVIEW FOR LOCATING THE FIRST SUCH PERSON FOR ME, AND I WILL PAY THE INDIVIDUAL \$1,000 TO DO THE 90-MINUTE TAPED INTERVIEW WITH ME, plus provide supporting evidence. And let me say, it will be the happiest check-writing session of my life. I DESPERATELY WANT TO BE PROVED WRONG. Mail me your (his) outline.

I am going public with this story because it is unlikely that any conventional news source will touch it, unless pressure is brought to bear. The reason is this: the problems are too horrendous even to be discussed by appropriate officials, unless they have specific answers. But they don't. What I present here cannot be smoothed over by a press release abount having set up a blue-ribbon study panel.

I literally stumbled into this information. I had read about one tiny aspect of it. I made a few extrapolations. Then I got worried. The problem looked as though it would have major implications. Little did I know!

Every dark cloud has a silver lining, they say. Well, every silver lining has its dark cloud. This is a "dark cloud" report about the high tech silver lining.

I am not trying to be deliberately gloomy, but this problem can only get worse, unless someone (and I don't know who) can figure out an answer. I don't like to present problems in REMNANT REVIEW for which I have no answers. This time I have to do what I don't like to do. If you've got some answer, WRITE!

I am hoping that by going to my reader I may locate one or more people who can provide decent counsel. Congress hasn't the foggiest idea of the threat that is now developing to the whole Western world. When I began this research porject, neither did I. Those who know the facts are so close to the problem that they may have grown jaundiced -- or else they are people who are the source of the problem, and they don't want it solved. The technicians remain silent, or discuss it only in "the inner circles" where the issues are understood. Policy-makers need to know.

ELECTRONIC AIDS (Part I)

Scenario: Paul Volcker is handed a telegram as he enters the monthly meeting of the Federal Open Market Committe. Every other member of the FOMC, which sets monetary policy for the U.S., is also handed an identical telegram. The telegram reads as follows:

THIS MORNING (a rural bank is named) SUFFERED A MAJOR FAILURE IN ITS COMPUTER SYSTEM STOP ALL DATA IN THAT COMPUTER HAS BEEN SCRAMBLED BEYOND RECOGNITION STOP WHEN BANK OFFICIALS ATTEMPT TO CALL UP THE RECORDS FROM ITS BACK UP COMPUTER TAPES THEY WILL FIND THAT THESE BACK UP TAPES ARE ALSO SCRAMBLED STOP ON MONDAY AFTERNOON THREE OTHER SMALL BANKS WILL SUFFER THE SAME FATE STOP ONE WILL BE IN NEW YORK CITY STOP ONE WILL BE IN LOS ANGELES STOP ONE WILL BE IN CHICAGO STOP PLEASE MEET AGAIN ON TUESDAY AFTERNOON STOP WE WILL GIVE YOU INSTRUCTIONS AT THAT TIME

Volcker calls the appropriate bureaucrat at the Federal Reserve Systems's headquarters, and he asks if there are any reports from the named bank. A few minutes later, the official calls back. The bank's management confirms the breakdown. The bank is attempting to install the back-up tapes. Volcker orders him to call back and stop the tapes from being installed. The bank complies. The tapes are then shipped to the Federal Reserve Bank under armed guard. When the FED's computer specialists acquire the same operating system and try to bring up the data, the system crashes. No usable data.

Tuesday morning, one by one three banks call the FED, the FDIC, and the Comptroller of the Currency's office, each with the same frantic tale. They have been working all night, but their computer records are scrambled. They cannot open at 10 a.m. They have only an hour to make a decision. What should they do? The FED instructs them to remain closed. They are also instructed to
keep their mouths equally closed.

The T.V. networks are tipped off, but no one at any bank says anything. Lines appear in front of each bank. Governers in all three states call frantically to Washington. They all remember Ohio and Maryland. What is the FED going to do?

The FOMC, the Board of Governors of the FED, each regional president, and a team of computer experts meet at the New York FED's offices. At three in the afternoon, a telegram is delivered to Volcker. It is brief. It says:

WORMS

"What the @%* is this?" he yells to no one in particular. The computer men turn white. They do their best to tell him what it means. They are finished answering his questions in about 45 minutes. Another telegram arrives. It says:

ON FRIDAY AFTERNOON THE CHASE MANHATTAN BANK WILL EXPERIENCE A SIMILAR COMPUTER FAILURE STOP ITS BACK UP TAPES WILL BE EQUALLY USELESS STOP IT WILL NOT BE ABLE TO REOPEN ON MONDAY MORNING STOP ON TUESDAY MORNING CITICORP WILL SUFFER A SIMILAR FAILURE STOP ON WEDNESDAY MORNING BANK OF AMERICA AND THREE OTHER MAJOR BANKS WILL ALSO SUFFER A BREAKDOWN STOP WE CAN PROVIDE YOU WITH THE CORRECTION FOR EACH COMPUTER STOP THE PRICE WILL BE THE REMOVAL OF DIPLOMATIC RECOGNITION OF THE ILLEGITIMATE STATE OF ISRAEL BY THE UNITED STATES AND AN END TO ALL ECONOMIC AID TO ISRAEL STOP TO PROVE THAT WE CAN DO THIS WE WILL SCRAMBLE ALL THE RECORDS OF CHASE MANHATTAN BRANCH BANK XYZ TOMORROW MORNING STOP

The next morning, all of the records of Chase Manhattan's branch bank are turned into random numbers. That afternoon, the President of the United States breaks off diplomatic relations with the state of Israel. The banks stay open. No crash of the data occurs. This time.

This is hypothetical scenario. It is NOT hypothetical technologically. This is the terrifying message of this issue the REMNANT REVIEW. what I have described here is conceivable technologically. On a small scale, it has already been threatened. Let's start with the historical and then go the the possible.

WORMS

Earlier this year, I read a very interesting article on a major problem racing computer software (programs) development companies. A program comes on one or more 5.25-inch plastic discs. It takes only a few seconds to copy a program on one disc to a blank disc which costs \$3. Yet these programs normally run at least \$250, and usually sell at \$495, and sometimes cost thousands. Very few are less than \$100. So you have a major temptation: make a \$500 asset out of a \$3 asset. Insert the \$500 program into drive A, write "COPY A:*.* B:" and hit the "enter key"; sixty seconds later, you have a \$500 program in drive B.

There are ways to make this copying more difficult. The companies code the programs, and force you to have a control disc in drive A at all times. These "copy protected" programs are a hassle for users. We cannot put them on a "hard (big) disc" easily, and sometimes the control disc dies for some reason. Then what? Your data are locked in your hard disc or on a floppy disc, but you can't get to the data because the control disc is not functioning. You order a replacement. Weeks go by.

Last year, several firms came up with a solution. It is called a WORM. A worm is a command which is built deep into the complex code which creates the program itself. These are incredibly complex codes, and it is easy to bury a command in them. They cannot be traced.

What does the worm do? It "eats" things. Say that you are a software thief. You make a copy of a non-copy-protected disc, either to use on a second computer, or to give (or sell) to a friend. The programs works just fine. But when the programs is copied to a new disc, the worm is "awakened." It bides its time, maybe for many months, maybe for years. The programs's user is blissfully unaware that a monster lurks inside his pirated program. He continues to enter data, make correlations, etc. HE BECOMES COMPLETELY DEPENDENT ON THE PROGRAM.

Then, without warning, the worm strikes. Whole sections of the data dispppear. Maybe the data storage disc is erased. Maybe it is just scrambled. Even his back-up data discs have worms in them. Everything he entered on those discs is gone. Forever.

Can you imagine the consternation of the user? He has become dependent on a booby-trapped program. His business could simply disappear. For the savings of \$500 (stolen program), he could lose everything he has.

Several firms threatened to insert worms into their programs. But then they backed off. They are afraid that lawsuits initiated against them might go against them in court. The could be hit for damages suffered by the thieving victims. Juries might decide that the punishment (a bankruptcy) was too much for the crime (a \$500 theft).

So far, no worms are lurking in any commercial software programs -- as far as I know and the industry knows, anyway. But what if a disgruntled programmer were to hide one in a master copy of, say, Lotus 1-2-3, the most popular business program on the market? What if ten thousand copies a month go out for, say, three years? Then, without warning, every company that has started using them loses three years of data? They sue Lotus. Lotus goes bankupt paying lawyers. NO COMPANY IN THE INDUSTRY IS WILLING TO TALK ABOUT THIS SABORAGE THREAT PUBLICLY. Obviously.

LARCENISTS

I just happened to stumble across an article on worms in a computer magazine. It occurred to me that it might be possible to use the worm technique as a form of deliberate sabotage rather that just as a copy protection device. But what did I know? I'm not a computer expert.

I know a computer expert, however. I mean, a REAL expert -- one of those people you occasionally read about. In the world of business, they're called "space cadets." They operate somewhere in between the asteroid belt and Jupiter. But this one is different. He's a businessman, too.

I got him to sit down with me to discuss the problem of worms. It turned out that he has a real fascination for the topic. He tells me that there are advanced design worms, called 'viruses' by 'hackers' -- computer freak programming genuises. "The software virus is the most terrifying thing I've ever come acr



Search RISKS using swish-e

Report problems with the web pages to the maintainer



Mark S. Day <<u>MDAY@MIT-XX.ARPA</u>>

To: RISKS@SRI-CSL.ARPA

Mon 9 Dec 85 14:57:40-EST

Hysterical panic about viruses in programs is at least as annoying as the more common complacent stupor about risks from computers. The author of <u>RISKS-1.27</u> seems to be dead set on Software Apocalypse Now. We swing from viruses in software to unencrypted data links on bank machines to teen-aged kids cracking systems. Also, the usual screams of "mad genius hackers playing sick games" can be heard... sigh, programmers are so misunderstood...

The discussion about viruses is actually sort of interesting, the others fall into the category of "there are fixes which have a certain cost; you have to decide whether it's worthwhile." Encryption and tighter security systems raise the cost of the system and also raise the cost of breaking the system. The question is, for the data and functions being provided, what is an appropriate level of protection? I'm not going to panic because many bicycles have cheap locks or no locks;

some bikes aren't worth stealing, and in some areas there's relatively little theft of bicycles. If I have data worth protecting, I should be prepared to protect it. I will agree that far too few people are aware of the hazards or of what they can do to protect themselves, but that is far from saying that I want to pay for security I don't need.

On viruses, etc.: it is certainly the case that you only want software which is written by people you trust (and ENTIRELY by people you trust -- see Ken Thompson's Turing Award Lecture for a further discussion of this). But is that different from needing to have bookkeepers and treasurers that you trust in order to avoid embezzlement? If bankers and national security types don't take steps to ensure that they have good software, then they certainly have a problem, but not a hopeless one. There have been previous proposals to have independent "software certification agencies" to ensure software quality, but I don't know if they would really be able to solve this problem.

The "solitary programmer" mentality is at least partly to blame for things like "unauthorized worms" -- if people expect to have their code read by others, who may question the reasons for doing certain things, it becomes enormously harder to conceal unauthorized features (unless the programmer can convince the inspector(s) to join in a conspiracy). I am still surprised at how many companies do not ask programmers to read each other's code. Quite apart from security worries, having inspections or walkthroughs seems to sharply improve maintainability and finds a number of bugs and design flaws.

I have little or no sympathy for people who illegally copy a program and then find one day that it's trashed their data. Serves 'em right.

--Mark

P.S. The term "worm" was not coined in a Scientific American column. I believe John Brunner used it in his novel The Shockwave Rider and Shoch and Hupp picked up the term for a paper in Communications of the ACM. It may have been used earlier than that; I don't know.

viruses, worms and history

Aaron M. Ellison <<u>BI467000%BROWNVM.BITNET@WISCVM.ARPA</u>> Mon, 09 Dec 85 08:56:27 EST

Regarding Neal Macklin's "expose" of virus technology, I would only add that the idea is not at all new. John Brunner, a well-known speculative fiction writer, wrote a novel called "Shockwave Rider" over 10 years ago(!) predicting the blackmailing of a then corrupt U.S. government by a morally-upright computer hacker. Although I share Neal's concerns, I am not at all convinced (even as a credit-card and ATM-card-carrying young and aspiring academic) that under certain circumstances, the collapse of the fractional reserve system, the banking system, and the credit markets would be an awful event. Sure there would be chaos, but who knows what could arise from the rubble. ...I would add that reading Shockwave Rider when I was in high school prompted me to learn about computers, and although I have not the competence to develop tapeworms and viruses, if it's just now getting out to the "hacker world" that viruses exist, you can bet that the NSA may already have developed one (pardon the paranoia).

Aaron Ellison Graduate Program in Ecology & Evolutionary Biology Brown University Providence, Rhode Island 02912

[The Worm Turns in His Gravy?]

< <u>TMPLee@DOCKMASTER.ARPA</u>> Sat, 7 Dec 85 22:25 EST

To: Neumann@SRI-CSL.ARPA [adapted for RISKS]

I suppose it would be nice to tell the original author of the long issue about viruses, etc., that there ARE technical solutions, although not necessarily within his lifetime if he's using IBM systems, which most financial institutions do ... Ted Lee

Re: <u>RISKS-1.27</u>

Dave Parnas <<u>vax-populi!dparnas@nrl-css.arpa</u> > Mon, 9 Dec 85 07:23:03 pst

Cc: nrl-css!neumann@SRI-CSL.ARPA

Peter,

Risks is supposed to be a digest. The huge article that just ate up my time like worm could have been digested and the summary put in a few lines. Worms have their place. Eating up stories like that one is one of their good uses. Worms digest waste.

Dave [and I got THREE copies of Dave's message. Oh, well. PGN]

✓ Electromagnetic Interference

Chuq Von Rospach <<u>sun!plaid!chuq@ucbvax.berkeley.edu</u> > Thu, 5 Dec 85 08:29:09 pst

I was listening to a radio station the other day whose studio is on the San Francisco Bay. In the early afternoon, the station started getting a re-occuring noise over the air that sounded vaguely like a burp, which distracted the DJ no end. It turned out after investigation by their engineers that it was being caused by a Navy Aircraft Carrier that had just entered the bay on the way to Alameda. Every time the radar pointed at the studio, it caused the stations electronics to go bonkers (that's a powerful radar...). I wonder what other electronics those things would interfere with?

chuq

[Perhaps the squawks were emitted by a carrier pitch-in? PGN]

🗡 crackers

Peter Reiher <<u>reiher@LOCUS.UCLA.EDU</u>> Wed, 4 Dec 85 22:30:33 PST

I imagine you will have numerous postings making the following point, but, if you don't, someone should say it.

> Thomas Cox writes:

>1. no password-protected system is EVER likely to be broken into by so-called

- > hackers. They can sit and guess, just like they can try and guess the
- > combination to my bike lock. I'm not worried about it.

This all depends on how loosely you define "stealing a password". Does a person who hangs around your printer room, picking up loose header sheets with people's account names and real-world names on them stealing passwords? Someone who does so can break into many systems, as many people will choose passwords equal to their login ids or first or last names. If the person communicated with people via email at your site, or was able to guess what their login id is (not a hard job in many places), then the same vulnerability exists. The problem is exacerbated if the cracker can get access to a list of your users. On most UNIX systems, once he is in at all, this is trivial.

[Not to mention the fact that passwords are usually transmitted unencrypted within local nets and externally as well... PGN]

In fact, barring fairly stringent rules on password choices, and/or physical security preventing intruders from accessing terminals (and, possibly, modem features to discourage brute force guessing), most computer systems can be broken into once a few user ids are known, provided the cracker has the modicum of expertise and equipment necessary to write a program to test all dictionary words against the user ids' passwords. The recent Bell Systems Technical Journal issue on UNIX had a discouraging article on how easy it is to break into the majority of UNIX systems, given a list of user ids, testing only twenty or forty possible passwords per user id.

Perhaps you don't consider a lax password system a password system at all, but, barring that, your statement is demonstrably false.

Peter Reiher reiher@LOCUS.UCLA.EDU {...ihnp4,ucbvax,sdcrdcf}!ucla-cs!reiher [Unfortunately, discussions of the risks of relying on passwords need to held over and over again. If you have not thought deeply or been burned, it is too easy to be naive. The sophisticated crackers -- as opposed to the simplistic ones -- find very few boundaries they cannot get through (or go around). PGN]

Ke: Hackers (aka "Head in the Sand")

Matt Bishop <<u>mab@riacs.ARPA</u>> 5 Dec 1985 0959-PST (Thursday)

I think Thomas Cox's article ("Hackers", <u>Risks V1N26</u>) is optimistic in the extreme:

- > 1. no password-protected system is EVER likely to be broken into by so-called
- > hackers. They can sit and guess, just like they can try and guess the
- > combination to my bike lock. I'm not worried about it.

Sorry, but I am. When you say "password-protected", I interpret that to mean the user setting his or her password to anything other than the site/manufacturer default. Turns out a lot of people set it to their name, login, spouse's name, etc. (See Morris and Thompson, "Password Security: A Case History", CACM 22(11), pp.594-597 (Nov. 1979) for more information about this claim.) If you know anything about the system you're attacking, such as whose account you're trying to get into, this makes the account rather a sitting duck. So I'd disagree with your statement above.

Of course, if you mean something else by "password-protected", could you be more explicit? My opinion could very well be inapplicable ...

(Incidentally, bear in mind the "bike" is worth maybe a half million, considering the information stored on it, so if you just trust the "lock", and don't take off a wheel, you're inviting trouble ...)

Matt

Hackers' guessing passwords

<> 8 Dec 1985 14:21:50 PST

From: Dave Dyer <DDYER@USC-ISIB.ARPA> To: risks@SRI-CSL.ARPA

In Response to Thomas Cox in Risks 1.26:

"1. no password-protected system is EVER likely to be broken into by so-called hackers. They can sit and guess, just like they can try and guess the combination to my bike lock. I'm not worried about it."

This is patently untrue. I have personally guessed passwords on

several occasions; It isn't even hard unless you want some particular password. One of the recent, widely publicised "hacker" cases involved exactly what you say is impossible; the perpetrator was merely making a sport of guessing passwords, and changing them as a warning to the account owner. In addition to guessing, there are multitudes of ruses to obtain passwords, some technical, but many simply exploiting human weaknesses.

It is certainly true that "unguessable" passwords exist, but any enforced mechanism for assuring unguessable passwords will also be regarded as "unrememberable", and therefore more vulnerable to non-guessing methods.

Hackers, Crackers, and Snackers

Peter G. Neumann <<u>Neumann@SRI-CSL.ARPA</u>> Mon 9 Dec 85 15:52:42-PST

To: RISKS@SRI-CSL.ARPA

I received an anonymous phone call this morning from someone who felt inspired by the last two issues of RISKS to relate some experiences he/she had had while working for the Texas Commerce bank. Apparently the computer maintenance staff had fun with the wire-transfer programs, using passwords that had been taped under a desk. They would randomly transfer various amounts (\$100,000 was mentioned as typical) from one account to anothe, just for kicks. They were astounded that no one every caught on, and the passwords were never changed. When I asked whether all such transactions had been reversed, the answer was probably yes.



Search RISKS using swish-e

Report problems with the web pages to the maintainer



Dave Platt <<u>Dave-Platt%LADC@CISL-SERVICE-MULTICS.ARPA</u>> Tue, 10 Dec 85 09:50 PST

Random-Quote: The race is not always to the swift, nor the battle to the strong -- but that's the way to bet. (DAMON RUNYON)

Recently, an increasing number of pharmacies have been putting greater amounts of drug information "on line". As I understand it, they will keep track of all of a particular customer's prescriptions, and will alert the pharmacist if they should be asked to fill a prescription that conflicts with any other medication that the customer is taking. The rationale is, I believe, that if a person is receiving prescriptions from two different doctors (different specialists, perhaps), then neither of the doctors would necessarily be aware of the drugs that the other had prescribed, or of any possible unfortunate interactions between the drugs. Normally, I assume that the pharmacist would inform the consumer and contact the prescribing doctor for further instructions.

Several concerns come to mind:

- Where is the database of drug conflicts derived from? Manufacturers' data files? FDA reports? Articles in recent medical journals? Just how complete is it?
- Does the database cover only drug-to-drug interactions, or is it more complete? Might it, for example, contain counter-indication information for specific drugs (e.g., don't take this if you're pregnant)? How about reports of unusual symptoms or side effects?
- How "intelligent" (sorry!) is the logic that compares a new prescription with a person's medical/drug history? Is there any Al/expert-system capability, or is it simply a look-up-a-list-of-conflicts? Might the code be capable of, for example, warning a person who's receiving medication for asthma not to take doses of a specific brand of antibiotic because that particular brand is preserved with a sulphite compound that has been reported to trigger asthma attacks in sensitive individuals?
- If a pharmacy advertises their new drug-checking software (and some do mention it in their ads), are they assuming any degree of responsibility or liability for either (a) false "conflict exists" warnings that cause a consumer not to take a necessary drug prescribed for them, or (b) any failure to alert a customer to a conflict that does exist?
- Will doctors, pharmacists, and/or consumers begin to depend on the correct functioning systems such as this, at the expense of studying the issues involved themselves?

This particular issue is similar to the one discussed several issues back, concerning AI/KE/expert-system tools such as MYCIN that "diagnose" illnesses from symptoms or "suggest" treatments. However, this system is one step further away from the doctor and closer to the consumer; there might be a greater tendency for people to "take it at its word" rather than simply using it as a tool.

SDI: Danny Cohen and Eastport Group comments

Jim Horning <<u>horning@decwrl.DEC.COM</u> > 11 Dec 1985 1340-PST (Wednesday)

[Forwarded With Permission from Gary Chapman]

Date: Tue, 10 Dec 85 16:14:34 pst From: Gary Chapman <PARC-CSLI!chapman@SU-Glacier.ARPA> Subject: Danny Cohen and Eastport group report

COHEN SAYS SDI CRITICS ARE "STAGNANT SUBCULTURE"

Danny Cohen, chairman of the so-called "Eastport group," told the Senate Armed Services Subcommittee on Strategic and Theater Nuclear Weapons that the discipline of software engineering is "an institutionalized and stagnant subculture." He said that Dave Parnas' criticisms were misrepresenting the facts by claiming that there are "scientific arguments" and "fundamental mathematical" obstacles that lead to the conclusion that reliable BM/C3 software cannot be built.

However, Cohen said in his testimony that the so-called "horserace" architecture studies have only paid "lip service" to potential battle management problems, and he criticized these studies harshly.

Cohen said that software engineers have a fetish with mathematical correctness, and that they "try to mimic mathematics at any cost, even if it means sacrificing functionality and relevance. This sect grossly overrates the perfection of Swiss clockwork, and strives to achieve it." Cohen said that the SDI should look to the telephone system as a model of a large system that works well with distributed, autonomous components. He said, "The communications approach copes with imperfections and corrects for them, rather than attempting to achieve an unattainable perfection."

Apparently the example of the telephone system is also featured in the first chapter of the Eastport group's report to the SDIO. A December 1 draft of the report was obtained by the editors of Military Space, and reviewed in the December 9 issue. The report's conclusions are summarized in the observation that computing resources and battle management software "are within the capabilities of the hardware and software technologies that could be developed within the next several years...with the tradeoffs necessary to make the software tractable in the system architecture."

The panel criticized the ten Phase 1 system architecture contractors for downplaying the problems of battle management software. The panel apparently recommends that the SDIO conduct a broader system architecture study, with an eye toward an "unconventional architecture whose program is within the anticipated limits of software engineering, without overreliance on radical software development approaches."

The panel rejects the "tight coordination" implied in the Fletcher Commission report of 1984. The panel recommends a loose coordination, with "robustness, simplicity and the ability to infer the performance of small parts of the system. Otherwise, the U.S. could not test a full-scale deployment short of actual use."

The panel also says in the report that "innovative approaches" are necessary for managing the software development of the SDI. The panel report recommends an independent research and technical support organization to supervise the program, and a high-speed communications network to support SDI contractors.

Cohen also told the editors of Military Space that he believes differences in opinion about the SDI within the computer science community come from different conceptualizations about the problem. Cohen said, "Critics like Parnas take the approach they're traditionally familiar with as software engineers--a 'waterfall' or 'top-down' approach. They look at battle management software as one single, gigantic 'bounded' problem requiring all-new software--instead of seeing it as a dynamic federation of many different networks and nodes, much of which may already be out there now.

"The implication of viewing battle management as a federated network--rather

than as a monolithic, rigidly centralized process prone to single-point software collapse and "Trojan horses'--comes down to this: the issue is not software, it's *protocols* between many different networks. It's inter-computer or inter-network communications--not single-system software."

🗡 Worms, etc.

"Keith F. Lynch" <<u>KFL@MIT-MC.ARPA</u>> Tue, 10 Dec 85 01:10:21 EST

To: MDAY@MIT-XX.ARPA cc: RISKS@SRI-CSL.ARPA

From: Mark S. Day <MDAY@MIT-XX.ARPA>

The "solitary programmer" mentality is at least partly to blame for things like "unauthorized worms" -- if people expect to have their code read by others, who may question the reasons for doing certain things, it becomes enormously harder to conceal unauthorized features (unless the programmer can convince the inspector(s) to join in a conspiracy).

I disagree. How does one guarantee that the source code shown is in fact what was compiled?

I have little or no sympathy for people who illegally copy a program and then find one day that it's trashed their data. Serves 'em right.

Does the punishment fit the crime? What if it was some employee who illegally copied the program, which then destroys irreplacable company data? How certain is it that this 'protection' scheme will not go off by accident? If it does, who is liable? Can the company which uses it simply disclaim all liability?

From: Aaron M. Ellison <BI467000%BROWNVM.BITNET@WISCVM.ARPA>

Regarding Neal Macklin's "expose" of virus technology, I would only add that the idea is not at all new. John Brunner, a well-known speculative fiction writer, wrote a novel called "Shockwave Rider" over 10 years ago(!) predicting the blackmailing of a then corrupt U.S. government by a morally-upright computer hacker. ...

The idea is older than that. I don't have any references, but I recall reading about 'computer viruses' before 1970. ...Keith

* `Gary North's Remnant Review' (Worms, etc.)

Stavros Macrakis <<u>macrakis@harvard.HARVARD.EDU</u> > Tue, 10 Dec 85 18:04:07 EST This overly-long message appears to say nothing new. We are treated to some sort of breathless and misinformed paranoia about `anti-Zionists', Soviets, and foreigners in general, not to mention hackers. We get thriller-novel political scenarios with countless pointless (and hardly verisimilitudinous) details. (See below for a textual analysis of North's tract.)

We all know that computer security is hard. We know that banks and other important institutions have often failed to apply even the most elementary security precautions. We even know about `trapdoors', `worms', and `viruses' (which were discussed during the design of Multics, if not earlier). We also know that both technical people and users of computers must become more aware of security issues.

What does North contribute?: a vision of a horrible secret hidden from the public by frightened bankers whose livelihood depends on hoodwinking the public into believing that paper money and bank deposits have value -- a secret which



Search RISKS using swish-e

Report problems with the web pages to the maintainer



Request for Cases, Settled or Decided

<<u>cole.pa@Xerox.ARPA</u>>

14 Dec 85 09:04 PST

There has been little legal analysis concerning the "computer revolution"; partly because there have been few cases that have been decided by the appellate courts.

I have started researching this area and would appreciate very much any pointers to cases -- threatened, settled, decided by trial and not appealed, or appealed -- that involve questions of:

(1) liability for unsuspected "bugs";

(2) liability for program design flaws;

(3) liability for disgruntled programmers taking "revenge" upon their corporation at the expense of the customers; or,

(4) liability for harm (personal or economic) caused by a human making computer-aided decisions. This could be anything from a medical decision using MYCIN, PUFF, ONCOCIN et. al. to an automobile designer using CAD/CAM.

I am not looking for situations where the vendor/programmer promised what he knew he could not deliver, outright fraud, or contractual disputes about the value delivered; I am trying to find situations where fault lay in the human-computer interaction.

There are a number of possible legal theories that may apply to the present range of problems; I also am examining theories that may apply as more "independant" and extensive AI applications, that involve less computer-friendly users, become part of everyday life. Some of these theories should extend to cover analagous situations; some will probably not; the questions I am interested in are WHY and HOW any theory should apply.

Again, I would be very grateful for any information from any of you. When this study is completed I will report that to this forum.

George S. Cole, Esq.

N.B.: This task is part of the research project I am working on while attending Stanford's C.S. Master's program, at Xerox PARC. I am a licensed attorney (temporarily suspending practice to gain the Master's Degree) and am extremely interested in attempts to combine the practices in these two fields.

Kisks of job displacement from computerization

"Fred Hapgood" <<u>SIDNEY.G.HAPGOOD%MIT-OZ@MIT-MC.ARPA</u>> Mon 16 Dec 85 07:24:18-EST

To: risks%MIT-OZ@MIT-MC.ARPA

Is anybody keeping track on an on-going basis, of the job categories being destroyed by the computer? A recent example is that of "presentation photographer" -- who, at the minimum, shot pix of graphs and graphics for presentations, and at the limit, designed and assembled those graphics. Not a big category, nor one with a set of skills whose loss leaves civilization that much poorer, but probably representative.

Anyway, I would very much like to reach the technology-andsociety scholar (surely there must be one somewhere) who is paying attention to this issue.

Kisks re computer-compared prescriptions

Richard Lamson <<u>rsl@RUSSIAN.SPA.Symbolics.COM</u>> Fri, 13 Dec 85 15:26 PST

Date: Tue, 10 Dec 85 09:50 PST From: Dave Platt <Dave-Platt%LADC@CISL-SERVICE-MULTICS.ARPA> Recently, an increasing number of pharmacies have been putting greater amounts of drug information "on line".

[...]

Several concerns come to mind:

- Where is the database of drug conflicts derived from? Manufacturers' data files? FDA reports? Articles in recent medical journals? Just how complete is it?

That's a very good question. It turns out that the database on drug interactions is very sparse, even for the simple case of two different drugs. There are a lot of common combinations which have never been adequately tested.

- Does the database cover only drug-to-drug interactions, or is it more complete? Might it, for example, contain counter-indication information for specific drugs (e.g., don't take this if you're pregnant)? How about reports of unusual symptoms or side effects?

Again, this database is also very sparse. Many drugs these days carry the warning that they haven't been tested in pregnant women, and therefore the physician should think twice (or more) before prescribing them to pregnant women (or those of "childbearing age", in many cases). One of the reasons drugs have not been adequately tested during pregnancy is that manufacturers are frightened of testing them in pregnant women, and, in fact, many drugs are not tested in "childbearing age" women at all, just in case they might be or become pregnant during the study!

Iegal bootlegs (a case against worms)

rich <<u>@CSNET-RELAY.ARPA,@case.CSNET:rich@rexago1.uucp</u>> Fri, 13 Dec 85 11:04:08 est

As I understand the paper work that comes with most micro software packages (big machine software is a different arena) what I buy is not a program but a right to use a given program. The mode of transmission is generally not specified. It could be my original distribution diskette, telephone, or a friend's legitimate copy.

If I scramble my original and then copy his, what have I done illegal? If I see a worm, you can bet my lawyer will hear about it.

K. Richard Magill

🗡 Passwords

mf <<u>ircam!mf@seismo.CSS.GOV</u> > Mon, 16 Dec 85 11:07:26 -0100 If you leave a \$500-bike locked and unattended for a week (as one of the readers put it) it is likely not to be there when you return, but not because a thief would have had the patience to try all combinations: he probably would wait for a quiet moment and break the lock or cut the chain.

And so it is with passwords: trying all possible combinations is theoretically feasible, but not very practical. A very simple method (and here the analogy with bikes stops) -- described for Unix but easily transportable -- is to run a [c]shell command file that fakes the login procedure, i.e., prints the login msg on a terminal, asking for the account and password (in no echo mode), and then printing "login incorrect" and exiting (after having recorded the password).

An unsuspecting user will think he mistyped his password and will try again. How does one protect against such booby traps?

verifying source code vs. executable code

"MARTIN J. MOORE" <<u>mooremj@eglin-vax</u>> 0 0 00:00:00 CDT [SIC!]

Re: Keith Lynch's question about knowing that the source code matches the executable, here is something simple that we did to support configuration control and to guard against EPROM decay when I worked at Cape Canaveral:

Whenever one of our programs was compiled and an executable file was generated, we ran a program to checksum the executable file (just a simple addition, but you could get much fancier with CRC if you wanted). This checksum was programmed into a fixed location in the EPROM. All of the programs contained code that, when the program was initialized, would run the same procedure on the program itself, compare the computed result to the stored result, and halt with an error message if there was a difference. Whenever a new program was installed, the stored checksum was recorded with the configuration control data, and the customer occasionally pulled surprise audits to make sure that the correct set of EPROMS was in use; they would come in, look at the stored checksum in the EPROM, and compare it to the recorded information. Since we had seven different instrumentation sites, each with slightly different configurations, and usually two or three versions of the program floating around, keeping track of the EPROM sets was a headache -- until we adopted this scheme, which worked beautifully.

If anyone wants specific details of the code (the processors were LSI-11s) I will be happy to send them to you.

Seminar - SDI Debate (SU)

Joan Feigenbaum <<u>JF@SU-SUSHI.ARPA</u>> Fri 13 Dec 85 17:56:01-PST

"SDI: How Feasible, How Useful, How Robust?"

This will be a technical debate, covering both hardware and software aspects of SDI.

Sponsor: Stanford Computer Science Department Date: December 19, 1985 Time: 8:00 p.m. Place: Terman Auditorium Organizer: Barbara Simons, IBM-SJ

Moderator: Dr. Marvin L. Goldberger, President of Cal Tech. Former member of President's Science Advisory Committee and Consultant on Arms Control and International Security.

Panelists:

Advocates:

Professor Richard Lipton, Professor of Computer Science at Princeton University, Current member of SDIO's Panel on Computing and Support of Battle Management.

Major Simon Peter Warden, the Special Assistant to the Director of the SDIO and Technical Advisor to the Nuclear and Space Arms Talk with the USSR in Geneva.

Opponents:

Dr. Richard L. Garwin, IBM Fellow and Adjunct Professor of Physics at Columbia University, Physicist and Defense Consultant.

Professor David Parnas, Lansdown Professor of Computer Science at the University of Victoria, Former member of the SDI Organization's Panel on Computing and Support of Battle Management.



Search RISKS using swish-e

Report problems with the web pages to the maintainer



✓ Enough on passwords? Pharmacy systems

"Elizabeth Willey" <<u>ELIZABETH%MIT-OZ@MIT-MC.ARPA</u>> Mon 16 Dec 85 18:00:52-EST

To: risks@SRI-CSL.ARPA

Could that discussion [on passwords] go over to SECURITY@RUTGERS (mail to SECURITY-REQUEST@RUTGERS to join)? Passwords have been discussed there before.

[It could. We have made the point that passwords are frequently misused. But everyone has an opinion on them, so it is only natural that there are lots of contributions on that subject! Actually, I rejected two messages on the subject for this issue, both of which would have required me to add caveats on the soundness of those messages. But there are still risks in relying on passwords that are worth including here. PGN]

About the pharmacy systems: people are essentially lazy. They will certainly become dependent on a computer program that tells them conflicts and stop noticing the conflicts themselves! Unless you formatted the program as a teacher, too: PHARMACIST, TWO OF THIS PATIENT'S CURRENTLY PRESCRIBED MEDICATIONS WILL REACT BADLY WITH THE NEW PRESCRIPTION. CAN YOU TELL ME WHICH ONES?

["Sorry. I did not know the answer, but I did not want to admit it

Re: Risks re computer-compared prescriptions

Brint Cooper <<u>abc@BRL.ARPA</u>> Mon, 16 Dec 85 20:52:56 EST

Risks of putting prescriptions "on-line" must be compared to the risks of NOT putting them on-line; i.e., to the risks of doing things as they now are done. It is tempting to compare them to the risks of doing things as we wish they were done, but this is unrealistic.

Now let's consider Dave Platt's well-founded concerns, keeping in mind that it is ALREADY the responsibility of the pharmacist to protect the patient/consumer from harmful drug interactions and the like:

The database of drug conflicts comes from wherever it now comes from. Package inserts (or the PDR) contain some of this information; this is mandated by law. Even if the automated database is less complete than the present human-maintained database, an automated system is much more likely to consult every relevant item. A human can forget!

Information beyond drug-drug interactions should be included if this is within the responsibility of the pharmacist. Otherwise, it should not be unless the medical and pharmaceutical professions consciously decide otherwise. Programmers should not redefine the practice of the professions of others.

Clearly, the first step is a non-intelligent database system. The example of an asthmatic taking another med containing sulphites should be covered by the database on medicine-medicine interactions.

Regarding degrees of responsibility, if the sources of information in the database are the same as at present, and if the pharmacist is using the database as a "decision aid," then I don't see how anyone's responsibility has been changed by a change in recordkeeping systems.

> Will doctors, pharmacists, and/or consumers begin to depend
> on the correct functioning systems such as this, at the expense of
> studying the issues involved themselves?

My problem with this question is that it assumes that doctors, pharmacists, and consumers presently study the issues involved. To the extent that an automated system provides a professional with free time, it will enable him/her to spend more time studying. But an automated system is not necessarily good or bad for anyone's habits!

Sure! People may come to rely on an automated Physician's Desk Reference (tm), but many people take their pharmacist's word as gospel right now. And too many pharmacists spend so much time as business managers selling cosmetics, stationary, motor oil, jewelry, books, and flowers that their "expertise" is anything but. At least a well-functioning database doesn't "forget" what it has learned.

Brint

Ø Oops!

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

To: "risks" <risks@sri-csl>

[I have abridged Marty's message. He pointed out that I did not complete the editing of <u>RISKS-1.30</u>, leaving the banner line as

RISKS-LIST: RISKS-FORUM Digest Thursday, 13 Dec 1985 Volume 1 : Issue 29 instead of

RISKS-LIST: RISKS-FORUM Digest Monday, 16 Dec 1985 Volume 1 : Issue 30 He also noted that "the table of contents seems to be rather skimpy this issue." (I left it out.) "I guess even RISKS is not immune to glitches!" (But it was a HUMAN error, not a computer-related error!) On the other hand, nobody complained that Friday the 13th fell on Thursday in RISKS-1.29, for those of you who remember Pogo. PGN]

[By the way, William Daul reported getting as many as 10 copies of <u>RISKS-1.29</u>. Another forum to which I belong recently had an issue where the system crashed repeatedly during mailing, and some users got as many as six copies, others getting none. I hope there is a way for the network people to fix this problem. PGN]

\$32 Billion Overdraft

Al Friend <<u>friend@nrl-csr</u> > Wed, 18 Dec 85 15:47:45 est

From: Al Friend - SPAWAR To: Risks Forum

Here is an interesting article out of the Washington Post. It seems that there is a very real potential for financial disaster lurking in the electronic banking jungle:

[Washington Post, 13 December 1985, p. D7]

Computer Snarled N.Y. Bank

\$32 Billion Overdraft Resulted From Snafu

By John M. Berry, Washington Post Staff Writer

The Bank of New York, the nation's 18th largest, had a brief \$32 billion

overdraft on its cash account at the New York Federal Reserve Bank when a computer failure last month snarled thousands of government securities transactions, a congressional committee was told yesterday.

By the end of the day, the overdraft had been reduced to \$24 billion, and the bank actually had to borrow that amount from the New York Fed -- pledging all of its assets -- in order to balance its accounts overnight.

Aside from the unprecedented scale of the borrowing, and the spillover effects on the government securities market, the incident intensified concern at the Federal Reserve over the vulnerability of the nation's financial payments system to a technological glitch that could have disastrous consequences.

Federal Reserve Chairman Paul A. Volcker and New York Fed President E. Gerald Corrigan went before a House Banking subcommittee yesterday to describe how the computer failure occurred and how the Fed and the bank dealt with the crisis it caused.

On Wednesday, Nov. 20, transactions involving more than 32,000 different government securities issues poured into the Bank of New York, one of the largest processors of such deals on behalf of others.

The bank's computer system was supposed to be able to cope with up to 36,000 issues, but a programming glitch developed and, unknown to anyone, the computer began to "corrupt" the transactions and make it impossible for the bank to keep them straight.

Because of the computer system breakdown, the bank could not instruct New York Fed where to send the securities arriving at the Fed on behalf of the bank's clients, and therefore could not get paid for them. The New York Fed was automatically taking money out of the Bank of New York's cash account to pay the sellers for the incoming securities, all of which are represented simply by computer records, rather than the familiar paper bonds still used by most corporations.

By Thursday evening, as hundreds of employes at a host of banks and government securities dealers tried to sort out the problems caused by the failure of the intricate and largely automatic network handling these transactions, the bank had a \$32 billion overdraft on its cash account at the New York Federal Reserve Bank.

The bank's computer specialists finally came up with a "patch" for its computer program -- a process described yesterday by its chairman, J. Carter Bacot, as the electronic equivalent of patching a tire -- that allowed it to begin to clear some of the backlog. But just after midnight, the patch failed too, after the overdraft had been whittled down to about \$24 billion.

The Fed kept both its nationwide wires for securities and cash transactions open in the early hours of Friday morning. When the patch failed, the Bank of New York was still able to borrow \$700 million from other banks. The rest was covered by a \$23.6 billion loan from the New York Fed. As collateral, the bank pledged all its domestic assets and all its customers' securities it was allowed to use for such purposes. Altogether, the collateral was worth #36 billion, according to the Fed.

The drama was not over. Around 5 a.m. Friday, the bank finally completed reconstruction of its customers' transactions from Wednesday. By 10 a.m., it had done the same for the Thursday deals. But, meanwhile, the rest of the government securities industry had begun its Friday activities, and securities and an overdraft were piling up again in the Bank of New York's account at the New York Fed.

"Faced with this situation," New York Fed President Corrigan told the

banking subcommittee, "at about 11:30 a.m., we temporarily stopped accepting securities transfers for the account of Bank of New York in an attempt to stabilize the situation somewhat and to see whether it was practical to prevent further increases in the overdraft without causing excessive disruption in the market more generally....

"Operationally, this meant that holders of government securities who had contracts to deliver those securities . . . to the Bank of New York for one of its customers [in return for payment] were temporarily unable to make delivery under those contracts," Corrigan said.

The stoppage lasted only for about 90 minutes that afternoon, and news of it did not spread widely for nearly an hour. Yet that disruption at the clearing bank was enough, Corrigan said, to make some market participants unwilling to trade securities among themselves. "Perhaps most importantly, there was also some evidence that investors were beginning to seek to break trades and financing transactions with dealers serviced by the Bank of New York."

Shortly after noon, the Bank of New York was able to begin handling the Friday transactions that had been piling up, and the Fed was again able to accept securities destined for the bank. By that point the bank was operating with a computer system that had undergone a major overhaul in less than 24 hours.

The crisis was over, but its final bill is still mounting.

The Bank of New York was out of pocket about \$5 million, an amount equal to about 7 percent of its earnings in the first nine months of this year, to pay interest on the money it had to borrow that Thursday.

It is still negotiating with many of the parties who may have sustained losses in transactions that were not completed on time. Such negotiations are common, said an official of one major securities dealer, because a few transactions are always going awry. This time it was thousands.

Some customers walked away in better shape. "Indeed, those individuals and intistutions who bought securities in question received a windfall in that they received interest for a day [on the securities], but did not incur any cost of financing," Corrigan noted.

But any loss or gain in dollars, even with millions of dollars at stake, is not the real issue. What worries both Federal Reserve officials and participants in the government securities market is the potential for a failure of the system.

On the average day, about \$200 billion worth of government securities transactions take place involving about 27,000 separate transactions, Corrigan said. Some days the totals are far larger.

"Like it or not," Volcker told the subcommittee, "computers and their software systems -- with the possibility of mechanical or human failure -- are an integral part of the payments mechanism. The scale and speed of transactions permit no other approach.

"In the last analysis, no mechanical system can be entirely 'fail-safe' and also be commercially viable," he said. "The costs would simply be too high, and the money and Treasury securities markets could not operate at the present level of efficiency."

The Fed chairman pointed out that, in this case, the Fed was available to lend the \$23.6 billion, on good collateral. "The effects in this instance were of unprecedented magnitude, measured by the amount of the overnight loan," he said. "But the effects in terms of market performance and risk were well contained. . . . I believe it would be wrong to overdramatize this incident."

Corrigan in his more detailed testimony sounded more notes of concern. "I believe our actions were prudent, disciplined and appropriate. In saying this, I should also confess that in some respects we were a bit lucky," he said.

Part of the luck was that the bank was able to get its computer going again as soon as it did. Another part, Corrigan said, was that Thursday was not an especially heavy day for securities transactions.

One government securities trader summed up the situation this way. "We're all afraid something will go bump and send the market into a tailspin.

... The Fed is working night and day to figure out what it can do. The banks are working night and day. But the amount of [trading] in financial markets is so large that we feel this is the No. 1 financial problem of the next few months. Banks have to be able to make settlements with each other."



Search RISKS using swish-e

Report problems with the web pages to the maintainer



* Can Bank of New York Bank on Star Wars? [PGN's retitling]

Jim Horning <<u>horning@decwrl.DEC.COM</u> > 20 Dec 1985 1413-PST (Friday)

Read <u>RISKS-1.31</u> only this morning. Found the detailed story on the Bank of New York fiasco extremely ironic. Last night in the debate at Stanford on the technical feasibility of the SDI, Richard Lipton chose the financial network as an example of the advantages of a distributed system (such as he is proposing for SDI) over a centralized one. "There have been no catastrophes." [What about the ARPANET collapse? PGN]

More generally, I am interested in reactions to Lipton's proposal that SDI reliability would be improved by having hundreds or thousands of "independent" orbiting "battle groups," with no communication between separate groups (to prevent failures from propagating), and separately designed and implemented hardware and software for each group (to prevent common design flaws from affecting multiple groups). He said that the SDIO/PCSBM panel had concluded that the integrated Battle Management and Command, Communcation, and Control (C3) software called for in the Fletcher Report could never be made trustworthy, but that a "meta-system" of simple, non-communicating components might be.

Jim H.

Cohen's AT&T SDI Software Analogy

Richard A. Cowan <<u>COWAN@XX.LCS.MIT.EDU</u>> Thu 19 Dec 85 19:04:45-EST

To: risks@SRI-CSL.ARPA

As pointed out at the SDI economic debate at MIT 11/19, all the other computer software systems (and predictions of technological failure that have proven wrong) were problems of man against nature. SDI software, as Parnas also pointed out, is a problem of man against man.

All historical analogies to SDI that involve successes in technological problems of man against nature are therefore worthless. If it were in the Soviet Union's vital interest to wreck the operation of the phone system, and they were willing to spend a few billion a year to do so, of course they could do it. (Remember how the mass Transit system in Tokyo was shut down by 50 terrorists a few weeks ago?)

By the way, the economic debate I referred to was quite interesting. Panelists were Bernard O'Keefe, CEO of Nuclear weapons contractor EG&G, Lester Thurow, MIT economist, and Leo Steg, former manager of GE's Space systems division. O'Keefe's company does Star Wars research, yet he ridiculed the Star Wars concept and pointed out the economic dangers. Thurow didn't give an opinion on Star Wars, but he pointed out the problems of diversion of talent, the new competition from other countries, and the fallacy of thinking that we can spend the Soviet Union into the ground. Steg was pro-technology, pro-SDI, pro-spinoffs. The Boston Globe had an article about it on the front page of the Business Section, (11/21), but I felt the article was shallow and biased.

If you'd like to judge for yourself, I have a TAPE of the discussion, AND a TRANSCRIPT. If interested, please contact me and I'll be happy to send you one of these (but you'll have to pay what it costs).

-Rich (cowan@mit-xx)

Failure probabilities in decision chains

Will Martin <<u>wmartin@BRL.ARPA</u>> Thu, 19 Dec 85 14:58:42 EST

One of our Directors has asked me to inquire about a reputed Bell labs study from 7 or so years ago, which he heard about at a conference. This study was on "failure probabilities"; one of the statements or conclusions he recalls was that if you have a string of five sequential decisions, one after the other, each based upon the preceeding, the reliability of the result is at the 59% level. I don't really have much other than this to go on, so, if this comment rings a bell with you, and you know the study (or studies) that this sort of conclusion came out of, I would greatly appreciate it if you could mail me a reference. If you know of work being done in this area by other organizations or particular researchers, any comments or rumors or hearsay or pointers to published work or theses would be welcomed.

If any documents related to this area of research exist on-line and are not proprietary, please feel free to mail me copies of anything you think might be relevant. The context of this is to provide some sorts of standards of comparison or generally-acceptable figures to use when evaluating the quality of a very complex and involved large software system.

Please e-mail responses to one of the addresses below. Thank you.

Will Martin US Army Materiel Command Automated Logistics Mgmt Systems Activity

UUCP/USENET: seismo!brl-bmd!wmartin or ARPA/MILNET: wmartin@almsa-1.ARPA

* Ten-year any-worseries [Plucked off the BBOARDS]

<> 19-Dec-1985 2140

From: Hoey@NRL-AIC (Dan Hoey)

hoey@NRL-AIC.ARPA 12/14/85 03:54:44 Re: Software alert: DATE-86 Received: from nrl-aic by MIT-MC.ARPA 11 Dec 85 10:59:57 EST Date: 11 Dec 1985 09:55:47 EST (Wed) From: Dan Hoey <hoey@nrl-aic.ARPA>

Early this year a message appeared on ARPANET-BBOARDS commemorating the ten-year anniversary of DATE-75. A somewhat more ominous anniversary will occur in four weeks, on 9 January 1986. Users of the TOPS-10 operating system should beware of software failures beginning on that date.

DATE-75 is the name of a set of program modifications applied to the TOPS-10 operating system, running on DEC PDP-10 computers. Before the modifications, the TOPS-10 system could only represent dates between 1 January 1964 and 4 January 1975. The DATE-75 modifications added three more bits to the representation of dates, so that dates up to 1 February 2052 could be represented. To maximize compatibility with existing software, the three extra bits were taken from several unused positions in existing data structures. The change was announced in mid-1974, and several tens of person-years went into updating software to recognize the new dates.

Unfortunately, reassembling these bits into an integer representing the date was somewhat tricky. Also, some programs had already used the

spare bits for other purposes. There were a large number of bugs that surfaced on 5 January 1975, the first day whose representation required the DATE-75 modification. Many programs ignored or cleared the new bits, and thought that the date was 1 January 1964. Other programs interpreted the new bits incorrectly, and reported dates in 1986 or later. Date-related program bugs were frequent well into the Spring of 1975.

On 9 January 1986, the second bit of the DATE-75 extension will come into use. Users of software developed in the 60's and early 70's on the TOPS-10 operating system should beware of problems with testing and manipulation of dates. Beware especially of programs that were patched after manifesting bugs in 1975, for in the rush to fix the bugs it is possible that some programs were modified to assume that the date was between 1975 and 1986. Any date that is off by a multiple of eleven years and four days is probably caused by this type of bug.

Dan Hoey

multiple digests as a result of crashed systems

Rob Austein <<u>SRA@XX.LCS.MIT.EDU</u>> Sat, 21 Dec 1985 13:50 EST

Once upon a time (when Rutgers.ARPA was flakey and I got five copies of SF-LOVERS in one hour), I discussed this problem with Mark Crispin (who maintains the Twenex mailer daemon, MMAILR). There are some real-world constraints that make it difficult to do things exactly as one would like here. I will use MMAILR for an example because it is the only mailer who's internals I have examined in detail.

Firstly, it is obviously preferable to send twice than to send not at all (in the general case anyway, obviously everybody has some examples of things they would rather not receive at all :-)), so typically the *last* thing that happens is that the message is marked sent and the queued disk copy either deleted or updated. So there's a window there during which a system crash will cause a duplicate. The size of this window is increased in MMAILR because it only does this marking on a per message basis, not a per recipient basis (ie, if you have a message that is going to 25 different recipients on different machines, the disk copy only gets updated after all the recipients have been tried). I was a little puzzled by this, so I asked Mark. The theory is that if your system is crashing a lot, the last thing you want to do is increase the amount of I/O to the disk copy of the queued message (thus increasing the chance that the system will crash while the update to disk is in progess, thus maybe trashing the message file). One could conceivably argue that the mailer should update between recipients when each recipient takes a non-negligable amount of time, but how do you know? Doing this for, say, Arpanet mail might be reasonable, but doing it for a fast local net wouldn't (it would spend most of its time doing disk I/O). Furthermore, for any given net the delay is a factor of the current load, which is

difficult to determine except by trying to use it. By this point you are spending more time trying to special-case your way around the problem than you are delivering mail, so you lose anyway.

One thing that might help prevent this sort of thing on a flakey system would be to delay startup of the mailer daemon for a little while after system boot. I expect that most of these cases of ten copies to a single person are cases where the system crashes within five or ten minutes of being rebooted.

--Rob



Search RISKS using swish-e

Report problems with the web pages to the maintainer



Brint Cooper <<u>abc@BRL.ARPA</u>> Mon, 23 Dec 85 17:38:18 EST

The idea of independent, non-communicating "battle groups" for an SDI system sounds great. But what about the "fratricide" problem?

Brint

Ke: Can Bank of New York Bank on Star Wars? [PGN's retitling]

<<u>Hibbert.pa@Xerox.ARPA</u>>

Mon, 30 Dec 85 12:00:25 PST

To: RISKS FORUM (Peter G. Neumann, Coordinator) <RISKS@SRI-CSL.ARPA> cc: horning@decwrl.DEC.COM (Jim Horning)

From: horning@decwrl.DEC.COM (Jim Horning)

Date: 20 Dec 1985 1413-PST (Friday) To: RISKS@SRI-CSL.ARPA Subject: Can Bank of New York Bank on Star Wars? [PGN's retitling]

Last night in the debate at Stanford on the technical feasibility of the SDI, Richard Lipton chose the financial network as an example of the advantages of a distributed system (such as he is proposing for SDI) over a centralized one. "There have been no catastrophes." [What about the ARPANET collapse? PGN]

The ARPANET collapse is a good contrasting case to show what Lipton was talking about. His point about the financial "network" is that it isn't a monolithic system, but a set of many (dozens?, scores?, hundreds?) independant systems. Any one of the systems could fail (even catastrophically) and it wouldn't be much of a problem for the whole system. ARPANet is a single monolithic system, centrally designed and administered. Most bugs manifest at exactly the same provocations at widely separated parts of the net.

There are at least a couple of separate national networks of automatic teller machines, and if any one of them dies, it shouldn't have any effect on the others, or on any of the banks with only local networks, or no networks at all. It would take a collapse of the phone system to put them all out of commission.

ARPANet on the other hand is a monolithic system. There is one protocol that all parts of the system must share, a common medium is used, and in there are only a few implementations of the protocols. It doesn't take much to blow the whole system out of the water. (For the most part it's as reliable as it is only because it gets constant use, and new parts aren't put in until they are shown to work most of the time.)

What Lipton was proposing at the Stanford debate was that we make an anti-missile shield from many separately designed and implemented parts so that their failure modes are more independant. This is a good idea, and if it were done, I would have plenty of faith in the system. However, that's not the way government gets things done. Since the DOD is running the program there's no way there would be more than three "separate" designs, and they would all go through the same approval process, removing many of the differences they started with.

Back to the ARPANet example, if you look at a larger system than just ARPA, including UUCP, DECNet, IBM's internal network, as well as the SOURCE, TYMNet, Compuserve, etc., you find the same robustness. ARPANet may die and be out of commission for a long time, and most people will still be able to get work done through some other medium, since only a fraction of the people using computer networks depend on any one of them.

Chris

Ke: Can Bank of New York Bank on Star Wars? [PGN's retitling]

Jim Horning <<u>horning@decwrl.DEC.COM</u> > 30 Dec 1985 1419-PST (Monday)

Chris,

I agree with many of your comments, and feel that the \$38 billion problem at Bank of New York is much more typical of how problems in nominally "independent" systems can propagate because of the intrinsic need to communicate. (As an example of a non-obvious interaction, recall its effects on the platinum futures market.)

In addition to the problems you cite, Lipton's scheme suffers from a few other flaws, including:

- The "simulation" that indicates that "only 5-10% extra bullets" would be needed apparently makes two dubious assumptions:

1) Independent "battle groups" (with sufficient "teraflops") can pinpoint targets as accurately as a cooperating distributed system.

2) Each "battle group" is able to recognize all "kills" by any battle group. I.e., the "extra bullets" counted are only those that are fired simultaneously at a target. With many of the proposed weapons, targets would be disabled, rather than disintegrated; with kinetic weapons, a single target could disperse to form a threat crowd.

(Note that observation of kills is a form of communication intrinsic to the problem.)

There were good systems reasons (completely outside of the computing requirements) that led the Fletcher commision to propose cradle-to-grave tracking (especially for RV vs. decoy discrimination) and a layered defense. Lipton gave no evidence of understanding those reasons, let alone making credible alternate proposals.

- The systems that you cite, and that he cited, are all ones where each component is in routine use under the exact circumstances that they must be reliable for. No matter how many independent subsystems the Lipton SDI is divided into, NONE of them will get this kind of routine use under conditions of saturation attack where reliability will be most critical. Thus there is a high probability that each of them would fail (perhaps in independent ways!).

Jim H.

Lipton and SDI

Herb Lin <<u>LIN@MC.LCS.MIT.EDU</u>> Mon, 23 Dec 85 18:09:59 EST

To: horning@DECWRL.DEC.COM

cc: LIN@MC.LCS.MIT.EDU, RISKS@SRI-CSL.ARPA

From: horning at decwrl.DEC.COM (Jim Horning)

More generally, I am interested in reactions to Lipton's proposal that SDI reliability would be improved by having hundreds or thousands of "independent" orbiting "battle groups," with no communication between separate groups (to prevent failures from propagating), and separately designed and implemented hardware and software for each group (to prevent common design flaws from affecting multiple groups).

That is absurd on the face of it. To prevent propagation of failures, systems must be truly independent. To see the nonsense involved, assume layer #1 can kill 90% of the incoming threat, and layer #2 is sized to handle a maximum threat that is 10% of the originally launched threat. If layer 1 fails catastrophically, you're screwed in layer #2. Even if Layers 1 and 2 don't talk to each other, they're not truly independent.

Mathematical The robot sentry

<<u>minow%rex.DEC@decwrl.DEC.COM</u> > Friday, 27 Dec 1985 13:11:28-PST

The following appeared on USENET net.general today (Dec 27). Martin.

"A much more sinister arrival on the robot scene is named Prowler. Created by Robot Defense Systems in Colorado, Prowler has been designed for use as a sentry to guard military installations, warehouses and other sites where security is important. When made available in the near future, this squat, sturdy, mobile device will carry microcomputers, software and sensors capable of locating intruders. Chillingly, buyers will be able to arm Prowler with machine guns and grenade launchers; they'll also be able to program the robot to fire at will. The manufacturer claims that interest in Prowler has been high, both among domestic companies who see it as a comparatively low-cost replacement for 24-hour human security, and certain foreign countries where government officials might prefer guards that will never revolt."

-- US Air magazine

-- JP Massar, Thinking Machines Corporation, Cambridge, MA

-- ihnp4!godot!massar, massar@think.com.arpa

-- 617-876-1111

Posted Fri 27-Dec-1985 16:08 Maynard Time. Martin Minow MLO3-3/U8, DTN 223-9922

Murphy is watching YOU

Rob Austein <<u>SRA@XX.LCS.MIT.EDU</u>> Mon, 23 Dec 1985 16:45 EST

About six hours after sending that message about mailers [RISKS-1.32], I found myself with the pleasant task of doing bit level reconstruction of XX's MAILQ: directory with DDT, because the system had crashed while MMAILR was in the middle of a disk transfer. Talk about ironic postscripts....

Cheers, Rob

Re: Failure probabilities in decision chains

Stephen Wolff <<u>steve@BRL.ARPA</u>> Mon, 23 Dec 85 17:33:15 EST

- * IF the overall decision is correct if and only if all five sub-decisions are correct, and
- * IF the sub-decisions are statistically independent, and
- * IF the probability that each sub-decision is correct is 0.9,
- * THEN the probability that the overall decission is correct is 0.9^5 = .59049 (vide any textbook in probability)

which is *suspiciously* close to "59%". But when Bill Walsh mentioned this problem to me in LA he was adamant that this was NOT the explanation he wanted. -s



Search RISKS using swish-e

Report problems with the web pages to the maintainer



X C&P Computer Problems Foul 44,000 D.C. Phones

Mike McLaughlin <<u>mikemcl@nrl-csr</u> > Sat, 4 Jan 86 13:52:34 est

(Excerpted from Washington Post, Friday, 3 Jan 86, pp D1 & D4) By Elizabeth Tucker, Washington Post Staff Writer

Up to 44,000 business and residential phone lines in the District (of Columbia) did not work or worked intermittently (Thursday, 2 Jan 86) because of computer problems at Chesapeake & Potomac Telephone Co. (C&P)

C&P... said the ... company had equipment trouble in its central office... between 2:20 and 4 pm. The problem was fixed when (the company) shut off connections to the 44,000 lines for a split second, and then turned the connections back on.

C&P has more than 780,000 phone lines in (DC).

(For) nearly two hours... customers often were unable to make or receive calls... The telephone company had not diagnosed the precise cause of the problem late yesterday....
Neither the White Hourse nor the General Services Administration... reported problems...

(GWU) Hospital experienced a delay in getting dial tones, but only for about 10 minutes...

...the Associated Press... could receive calls but not make them between 2 and 4 pm....

"You don't know what's going on in terms of news... I thought someone cut the cables. I was worried." (AP spokesman)

The Washington Post Co. also experienced problems...

One State department official ... "... heard corridor gossip [that people] weren't getting calls in or out."

The DC police... reported no problems in receiving 911 emergency calls, and sid there was no appreciable drop off in calls... C&P... said some people may have experienced problems reaching 911... "It could be that no one had problems with 911."...

The problem is not considered usual... "They don't know what caused the problem, but it's up and working fine . . . For all intents and purposes they reset the system, turned off all the connections and then turned them back on again -- LIKE RESETTING A COMPUTER." (EMPHASIS supplied)

"They are researching and analyzing the tapes to see what caused the problem."... such problems can occur when heavy calling is taking place ... but that such was not the case (2 Jan 86).

"We ruled it out . . . A lot of people aren't working downtown... calling volumes are down dramatically." The telephone system "sometimes can get confused," and think there is heavy calling when there isn't...

###

(parentheses and close up ... are mine) [brackets and spaced . . . are the Post's, as are "quotes"] I restrained myself from editorial comments, except where I just had to go

all caps for emphasis. Mike McLaughlin

Putting the Man in the Loop

"Jim McGrath" <<u>MCGRATH@OZ.AI.MIT.EDU</u>> Thu 2 Jan 86 21:43:54-EST

I found the calculations involving SDI reliability interesting. As well the debate on SDI software. But it appears as if people may be making some aspects of the problem too hard. Hoping that I have not missed this part of the conversation....

Obviously some problems (precise aiming of weapons for instance) demand computer control. And the time constraints involved in boost phase interception may require computer control. But other aspects (such as initial activation of weapons for mid-course and terminal phase interception, target discrimination, neutralization of counter-measures) could be made with substantial human input. Thus no need for monster AI programs to cope with all possible contingencies humans are ready made for that purpose.

The model to think of is a sophisticated computer game. The human operator(s) would take care of truly strange cases (rising moons,

flocks of interplanetary geese) and either determine strategy and/or provide input parameters for the actual computer controllers (e.g. "Looks like they are using dummy decoys of the DUMDUM class - better change certain probabilities in your expert systems target discriminator in the following manner"). The trade off here is decreased reliance on sophisticated AI programs that we all concede that state of the art is not capable of producing and increased reliance on software that provides an excellent interface to the human operator. That would seem to be the easier task (we already have experience in designing control systems for high performance jet fighters).

Of course, this increases the problems associated with real time secure communications, but you were going to have to face them anyway.

Jim

Testing SDI

"Jim McGrath" <<u>MCGRATH@OZ.AI.MIT.EDU</u>> Thu 2 Jan 86 21:45:01-EST

From Risks, Volume 1 : Issue 33:

> From: horning@decwrl.DEC.COM (Jim Horning)
> The systems that you cite, and that he cited, are all ones where each
> component is in routine use under the exact circumstances that they
> must be reliable for. No matter how many independent subsystems the
> Lipton SDI is divided into, NONE of them will get this kind of routine
> use under conditions of saturation attack where reliability will be
> most critical. Thus there is a high probability that each of them would
> fail (perhaps in independent ways!).

This seems to be a common problem with any modern weapon system (or even not so modern - it took WWI for the Germans to realize that the lessons of the 1880's concerning rapid infantry fire (and thus the rise of infantry over calvary) did not take artillery development adequately into account). But this might be easier to manage than most.

What if, after suitable advance notice, the SDI system was fully activated and targeted against one of our periodic meteor swarms? While not perfect targets, they would be quite challenging (especially with respect to numbers!), except for boost phase, and CHEAP. If the system was regenerative (i.e. you only expended energy and the like), then the total cost would be very low.

Meteors are just a casual example. My point is that the costs of partial (but system wide) testing does not have to lie with the targets (which many people seem to assume) as much as with weapons discharge - which may be quite manageable.

Jim

Independent Battlestations

"Jim McGrath" <<u>MCGRATH@OZ.AI.MIT.EDU</u>> Thu 2 Jan 86 21:45:43-EST

From Risks, Volume 1 : Issue 33:

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

<> From: horning at decwrl.DEC.COM (Jim Horning)
<> More generally, I am interested in reactions to Lipton's proposal that
<> SDI reliability would be improved by having hundreds or thousands of
> "independent" orbiting "battle groups," with no communication between
<> separate groups (to prevent failures from propagating), and separately
<> designed and implemented hardware and software for each group (to
<> prevent common design flaws from affecting multiple groups).
> That is absurd on the face of it. To prevent propagation of failures,
> systems must be truly independent. To see the nonsense involved,
> assume layer #1 can kill 90% of the incoming threat, and layer #2 is
> sized to handle a maximum threat that is 10% of the originally
> launched threat. If layer 1 fails catastrophically, you're screwed in
> layer #2. Even if Layers 1 and 2 don't talk to each other, they're

True but his solution WOULD reduce the probability of the propagation of "hard" errors (i.e. corrupting electronic communications), and the whole independence approach should lead to increased redundancy so as to deal with "soft" propagation of errors such as you cite.

Remember, you do not need to PREVENT the propagation of errors, just reduce the probability enough so that your overall system reliability is suitably enhanced. I think the approach has merit, particularly over a monolithic system, and should not be shot down out of hand.

Jim

Re: Failure probablities in decision chains and decision independence

<

🖣 🛖 🕨 🗊 🖉 🐨 🚀

Search RISKS using swish-e

Report problems with the web pages to the maintainer



Jim Horning <horning@decwrl.DEC.COM> 4 Jan 1986 1536-PST (Saturday)

Jim,

Thanks for your comments. However, I do have to disagree with your cheerful assessment of the chances for REALISTIC testing of any SDI system or major subsystem. The problem is not that there is no testing that could be done, but that any substantial change in the system's environment is likely to provoke a new set of unexpected behaviors.

Certainly, an SDI that failed to shoot down a meteor swarm could be judged faulty. (And certainly any experienced software engineer would predict that it WOULD fail to shoot down its first meteor swarm.) But what reason is there to believe that an SDI that had shot down every meteor swarm since its deployment would act in the intended manner when faced with a full-scale nuclear attack, which would certainly be accompanied by both attacks on the SDI system itself and by extensive counter-measures?

It is in the nature of counter-measures that you cannot be sure in advance that you have full knowledge of the counter-measures that your opponent will throw at you--especially in a first engagement. Thus, there is in principle no way to adequately test your system's response to counter-measures.

It is in the nature of distributed and real-time systems that the most catastrophic failures tend to come in periods of heaviest load. Thus the results small-scale testing can't be extrapolated with confidence.

It is in the nature of destructive testing (which a full-scale nuclear attack on an SDI certainly would be) that you can't test the thing that you will ultimately rely on. However, it had better be something so assuredly similar to the ultimate system that you can be confident in the extrapolation.

Finally, one brief non-software point: I read a column the other day (Tom Wicker?) that pointed out that every technology that would be effective against ballistic missiles would be far more effective, far sooner, as an anti-satellite system, since the behavior of satellites is more predictable, and the attacker can pick his moment. Even without SDI, the US is far more dependent on satellites for both defense and civilian uses than the USSR. And any space-based SDI would make a very tempting ASAT target. So developing the technology needed for the system INCREASES the risk of relying on the system.

Jim H.

Ke: Meteors as substitutes for nuclear war

Dave Parnas <vax-populi!dparnas@nrl-css.arpa> Sat, 4 Jan 86 16:50:35 pst

Cc: nrl-css!horning@decwrl.ARPA

The comments that you reported on testing SDI, proposing that we test it by shooting at periodic meteor swarms make me wonder how many of the people in our profession have trouble discriminating between real problems and arcade games. Shooting at an easily predictable non-evasive meteor has about the same relation to the real job of SDI as shooting at a target in a booth at a county fair has to shooting at woods in heavy brush from a moving airplane. If I had a computer program that had been tested by controlling a weapon at a county fair, I would not have much confidence in its performance the first time that the B.C. Government tried to use it in its periodic wolf kills from light planes. In fact, I hope someone sells that idea to them.

Dave

Re: Putting a Man in the Loop

Jim McGrath <J.JPM@Epic> Sat 4 Jan 86 19:24:35-PST

From: Herb Lin <LIN@MC.LCS.MIT.EDU> [Date: Sat, 4 Jan 86 18:52:04 EST] [Herb's message is embedded. PGN]

From: Jim McGrath <MCGRATH at OZ.AI.MIT.EDU> The model to think of is a sophisticated computer game. The human operator(s) would take care of truly strange cases (rising moons, flocks of interplanetary geese)..

But the major problem is not the things that the computer isn't sure about, but rather the things that it is sure about that are not true. How would the human ever know to intervene?

I thought a bit about that, and have a suitable elaboration. Basically, you require a "two key" system, with the computer holding one key and a human operator/monitor another. This is primarily for the "go/no go" decision. After an attack is acknowledged, you concede the possibility of overkilling by the computer (taking out third party satellites and the like) in return for the more immediate response to attack provided by the computer.

This takes care of the computer going off half cocked. If you are worried about the computer missing an actual attack, you can now set the sensitivity low, trusting to the human monitor to not activate when appropriate.

Actually, this is too simple. What you really want is to have the hardware/software under a set of human operators, perhaps partitioned to provide zone coverage. The humans act as before, mainly as checkpoints for activation decisions, overseeing strategy, sending expert information to the computers as the situation unfolds so that the software does not have to be a tactical genius. Now a set of human supervisors sit on top of the operators. They have another "key," and so can break ties on activation decisions (or even override lower level decisions). Their other missions are to advise operators on developing strategy, keep the command authorities informed, and to act as "free safety." That is, they will have the authority to override operator commands so that targets that find seams in the zones (or similarly defy the operator/computer teams) will be

targetted for attack. Normally they will access information at a much higher level than an operator (the former will have to deal with thousands of targets - the latter tens of low hundreds).

Other concepts can be advanced: advance/retard the ease of a go/no go decision according to alert status and the like. The main point is that a man in the loop is a big win, since you get a proprogrammed general purpose computer which can take care of those "higher level" decisions. Response time is not a concern - seconds are not vital if you have 20 minutes. Only for boost phase interception do you run into difficulties.

Jim

Re: Putting a Man into the Loop

Jim McGrath <J.JPM@Epic> Sat 4 Jan 86 21:47:31-PST

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

"go/no-go"

You mean fire/don't fire?

I mean weapon activation. Firing decisions for specific targets will be made by computer, but the weapons themselves will be inert until activated.

After an attack is acknowledged, you concede the possibility of overkilling by the computer (taking out third party satellites and the like) in return for the more immediate response to attack provided by the computer.

So your solution is that you kill everything, and don't do discrimination?

No. I meant exactly what I said. You concede that you might make a mistake in firing (which was your original objection). You do not aim for making a mistake. I explicitly said in the same message that one of the jobs of human operators is to assist in real time parameter adjustment so that the computer controlled weapons would be able to discriminate better.

As I said earlier, boost phase poses a particular problem. The only thing I can see to do now is to trust in AI to give you a good initial screen, and to argument this with a human authorized to override the problem in a few seconds. This could work well for limited periods of time (such as alerts), but I have problems with it for extended periods.

Jim

🗡 Testing SDI

Herb Lin <LIN@MC.LCS.MIT.EDU> Sat, 4 Jan 86 18:54:43 EST

From: Jim McGrath <MCGRATH at OZ.AI.MIT.EDU>

This [full-scale system testing -- HL] seems to be a common problem with any modern weapon system (or even not so modern - it took WWI for the Germans to realize that the lessons of the 1880's concerning rapid infantry fire (and thus the rise of infantry over calvary) did not take artillery development adequately into account).

And there have been disasters. Only here, the disaster is bigger.

What if, after suitable advance notice, the SDI system was fully activated and targeted against one of our periodic meteor swarms? While not perfect targets, they would be quite challenging (especially with respect to numbers!), except for boost phase, and CHEAP. If the system was regenerative (i.e. you only expended energy and the like), then the total cost would be very low.

Interesting example, but problematic. No kill assessment for one, under some circumstances. Entirely different signatures for another.

Meteors are just a casual example. My point is that the costs of partial (but system wide) testing does not have to lie with the targets (which many people seem to assume) as much as with weapons discharge - which may be quite manageable.

But if the tests are to be realistic, then the right targets are essential, especially since a counter-measure is to try to fool with

🗡 Testing SDI

Herb Lin <LIN@MC.LCS.MIT.EDU> Sat, 4 Jan 86 22:45:25 EST

From: Jim McGrath < MCGRATH at OZ.AI.MIT.EDU>

remember that the major cost of the target simulation is in the boost phase. Once the targets are in sub-orbit, it makes no difference whether they were fired independently by hundreds of expensive boosters or were accelerated from orbital velocity, after having been place there originally through more economical means. Terminal phase tests are especially easy to do this way. Only boost phase is intrinsically expensive.

I agree with your technical point. But successful boost phase is what

SDI is all about. The technology for dealing with mid-course and terminal is ALREADY here. You need boost phase so that you can thin out the midcourse and terminal.

Re: Testing SDI

Jim McGrath <J.JPM@Epic> Sat 4 Jan 86 19:36:57-PST

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

From: Jim McGrath <MCGRATH at OZ.AI.MIT.EDU>

What if, after suitable advance notice, the SDI system was fully activated and targeted against one of our periodic meteor swarms?

Interesting example, but problematic. No kill assessment for one, under some circumstances. Entirely different signatures for another.

It would test some aspects of the system on a system wide level (such as detection and tracking), and would even provide good kill estimates in some cases (KE weapons and small targets). But as I said:

Meteors are just a casual example. My point is that the costs of partial (but system wide) testing does not have to lie with the targets (which many people seem to assume) as much as with weapons discharge - which may be quite manageable.

But if the tests are to be realistic, then the right targets are essential, especially since a counter-measure is to try to fool with the targets that the defense sees.

True, but remember that the major cost of the target simulation is in the boost phase. Once the targets are in sub-orbit, it makes no difference whether they were fired independently by hundreds of expensive boosters or were accelerated from orbital velocity, after having been place there originally through more economical means. Terminal phase tests are especially easy to do this way. Only boost phase is intrinsically expensive.

(That's two messages where I've come up with approaches to problems that work on all phases except boost phase. Although initially attractive, perhaps concentrating more on mid-course and terminal defense will ultimately prove more beneficial.)

Jim

Independent Battlestations

Herb Lin <LIN@MC.LCS.MIT.EDU> Sat, 4 Jan 86 18:59:03 EST > From: Herb Lin <LIN@MC.LCS.MIT.EDU>
<> From: horning at decwrl.DEC.COM (Jim Horning)
<> More generally, I am interested in reactions to Lipton's proposal that
<> SDI reliability would be improved by having hundreds or thousands of
> "independent" orbiting "battle groups,"..
> That is absurd on the face of it. To prevent propagation of failures,
> systems must be truly independent. To see the nonsense involved,
> assume layer #1 can kill 90% of the incoming threat, and layer #2 is
> sized to handle a maximum threat that is 10% of the originally
> launched threat. If layer 1 fails catastrophically, you're screwed in
> layer #2. Even if Layers 1 and 2 don't talk to each other, they're
> not truly independent.

True but his solution WOULD reduce the probability of the propagation of "hard" errors (i.e. corrupting electronic communications), and the whole independence approach should lead to increased redundancy so as to deal with "soft" propagation of errors such as you cite.

Remember, you do not need to PREVENT the propagation of errors, just reduce the probability enough so that your overall system reliability is suitably enhanced. I think the approach has merit, particularly over a monolithic system, and should not be shot down out of hand.

This is the fundamental point of disagreement. If SDI is just another defensive system, then all that you say is right. But it isn't. I will stop beating the perfect system horse when the SDI supporters acknowledge that large-scale population defense can never be made certifiably reliable.

Re: Independent Battlestations

Jim McGrath <J.JPM@Epic> Sat 4 Jan 86 19:52:46-PST

What do you mean by "certifiably reliable?" While politicians may talk about 100% reliability, we are all scientists and engineers here - we know that nothing, including such things as the sun rising, is 100% reliable. You must really mean X% reliable, where X is a high number (perhaps high enough so as to reduce to a very low probability the chance of a single warhead getting through). In that case, independent battlestations, and other measures, might give you the number you need. I submit that it is too early to dismiss these approaches out of hand, since you are really talking about a quantative difference and we do not have good numbers yet.

Anyway, I am arguing for a highly reliable, but by no means perfect, system. My X would probably be lower than yours. I really do think that there is a difference between a few million dead (horrible, on the scale of WW II) and hundreds of millions dead (utterly unprecedented). And while I am certain that we all, including the public, would like as high an X as possible, they would agree that

losing a city or two and some missile bases/airfields would be a lot better than losing everything.

Besides, complaints that politicians are lying do not sit well with me. Of course they are lying. WE WANT THEM TO LIE. Politicians who tell the truth get kicked out of office. Our entire posture of extended deterrence is a joke, since we do not have the capability to creditably back it up. But you try to get someone elected promising to reinstate the draft, raise the defense budget further, or pull back our troops and cut Europe/Japan loose.

We have to make do with what we have.

Jim

[Do we have to have it just because we can make do with it? PGN]

Independent Battlestations

Herb Lin <LIN@MC.LCS.MIT.EDU> Sat, 4 Jan 86 23:03:58 EST

From: Jim McGrath <J.JPM at Epic>

What do you mean by "certifiably reliable?"

A system whose performance is known in advance to be adequate to the task. I don't care if the number for reliability isn't 100%, just high enough so that no one dies.

We all, including the public, would like as high an X as possible, they would agree that losing a city or two and some missile bases/airfields would be a lot better than losing everything.

But that is not the goal of the SDI.

Besides, complaints that politicians are lying do not sit well with me. Of course they are lying. WE WANT THEM TO LIE. [...]

We have to make do with what we have.

So you condone lying to the public as a tool of public policy? How would you like to acknowledge that publically in a letter to the NY Times? Don't forget to add that you support SDI, and that truth doesn't matter when you try to justify a weapon system -- never mind what it actually does. We can say that we will spend millions of dollars on AIDS research since that will save lives, and spend the money instead on nerve gas, which will also help to eliminate AIDS (by killing homosexual soldiers).

Sorry; I believe that elected leaders have a responsibility to tell

the truth to the public, and to educate them away from fairy tales. I would rather see precious defense dollars go to create good anti-tank weapons; that would have some chance of improving extended deterrence.

Mathe The Goal of SDI

Jim McGrath <J.JPM@Epic> Sat 4 Jan 86 21:52:13-PST

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

We all, including the public, would like as high an X as possible, they would agree that losing a city or two and some missile bases/airfields would be a lot better than losing everything.

But that is not the goal of the SDI.

Which does not mean it should not be supported for that reason. Most government programs have consequences (sometimes good, sometimes bad) never conceived of in their initial purpose. That does not mean you ignore them when evaluating the program.

I simply do not follow your logic at all. Do you want to score points against Reagan and Company? Or do you want to discuss strategic defense, and SDI as it is developing? I'm not interested in defending Reagan, just developing defense and seeing that it is done the best way possible.

Jim

Politicians

Jim McGrath <J.JPM@Epic> Sat 4 Jan 86 22:12:56-PST

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

Besides, complaints that politicians are lying do not sit well with me. Of course they are lying. WE WANT THEM TO LIE. Politicians who tell the truth get kicked out of office....

So you condone lying to the public as a tool of public policy? [...]

You are arguing from emotion (almost hysterically), not reason, which I do not expect of you. I stated a fact: public officials must lie on many (not all) issues in order to retain office. (I could have said "evade," or just "keep quiet about" if the word "lie" hits you so hard - I see no functional distinction.) This is one thing that everyone, no matter what their policy perspective, agrees on (this comes from several graduate seminars, and personal experience). I did not say that I liked that state of affairs much. But I do not find it reasonable to blame the politicians. Rather, the fault lies with the voters.

Unlike many of my friends in the social sciences, I do not concentrates on the "oughts" of the world. I focus on the empirical evidence. Perhaps it is the scientist in me. So when I observe a political system that punishes frank and honest talk about some issues (usually those, like nuclear war and taxes, that are too horrible to contemplate), I acknowledge this as a fact, and do not waste time decrying it. My decrying it is not (to the first approximation) going to change human nature. Thus my comment "we have to make do with what we have."

Sorry; I believe that elected leaders have a responsibility to tell the truth to the public, and to educate them away from fairy tales. I would rather see precious defense dollars go to create good anti-tank weapons; that would have some chance of improving extended deterrence.

Come on now. Leaders can only lead where people are, ultimately, willing to go. Just look at the nuclear freeze movement. This is the level at which the public thinks of nuclear war when it is forced to think.

Finally, your last sentence shows that you missed my entire point. Congress (i.e. the people) will not budget for the necessary increases in conventional weapons (let alone the Europeans). Ultimately it does not matter what you or I like, it is what the people will accept. And if they act "irrationally," then I feel we cannot just sit back and demand that out "leaders" make them change their minds, or that the people change their stripes. Instead we should focus on the possible - which is, afterall, what politics is all about.

Jim

Re: Pharmacy prescription systems

<Hoffman.es@Xerox.ARPA> 5 Jan 86 17:52:32 PST (Sunday)

Not speaking legally, but just morally, I think any professional who relies on a single source of advice when more are available is derelict. In any life-critical situation, information should always be tested or cross-checked whenever possible.

Would you exonerate a pharmacist (or a physician, for that matter) who relied completely on a particular reference book which had a critical error in it? Or on the tape-recorded lecture of some (human, less-than-perfect) instructor? Or, in the case under consideration, on some expert computer system? I certainly wouldn't.

The pharmacist does not shoulder all the moral burden in this

hypothetical case. Some of it belongs to the information source (publisher, human instructor, or expert computer system). Just not all of it. As the other commenters on the subject have noted, the user must be carefully trained against unthinking dependency. That's the single most important factor.

This is another instance of the urgent necessity to debunk the popular myth of computer infallibility. People are all too eager to stop thinking and let others (parents, teachers, priests, politicians, computers) make all their decisions. And the others usually love the role, too. In the case of computer systems, we their builders are in this seductive position and we must remember the inherent perils.

--Rodney Hoffman

How to steal people's passwords

Roy Smith <allegra!phri!roy@seismo.CSS.GOV> Sun, 5 Jan 86 16:56:19 est

In Volume 1, Issue 34, nelson@uw-beaver.arpa talked about faking login procedures and non-system software masquerading as system software. Well, an interesting thing just happened to me along those lines.

We've got several modems used for both dial-in and dial-out. To place an outgoing call, you disable logins on a line (a program, acucntrl does this for you) and use kermit to talk to the modem. I had just done this when somebody called in. The modem, of course, didn't know logins were disabled and answered the phone.

At this point, nothing much prevented me from pretending to be a login process and prompting the unsuspecting user for his login name and password, then faking a burst of noise and breaking the connection so s/he wouldn't suspect anything out of the ordinary.

Our PBX allows you to forward all your calls by dialing "12 NNN". Until canceled, all incoming calls get routed to xNNN. I could have had the modem forward all its calls to my office phone. Plug an Apple-II w/modem into my phone line, and I'm all set to steal passwords for a night. Fix it up in the morning, and nobody would suspect anything worse than a modem temporarily going bonkers, which happens often enough.

Roy Smith <allegra!phri!roy> System Administrator, Public Health Research Institute 455 First Avenue, New York, NY 10016



Search RISKS using swish-e

Report problems with the web pages to the maintainer

The Risks Digest Volume 1: Issue 35



PLEASE READ Weapons and Hope by Freeman Dyson.

Peter Denning <pjd@RIACS.ARPA> Tue, 7 Jan 86 10:26:44 pst

A number of correspondents have brought up points analyzed in great detail and with great clarity by Dyson in WEAPONS AND HOPE. Examples: Dyson argues against building cases for or against particular defense systems by counting the dead or the living. The number who may survive or die is incalculable and arguments based on such calculations are meaningless. Dyson analyzes in some depth the fact that satellites are easy prey compared to missiles. His objections to Star Wars have little to do with the technical points raised by most computer scientists. They are based on an analysis of many possible U.S. strategic strategies arrayed against Soviet and other strategic strategies. Dyson believes that there is a place for nonnuclear ABMs in a nuclear free world, an argument that CPSR should familiarize themselves with (CPSR has issued position statements against SDI based on the premise that SDI is nothing more than an ABM system). Dyson argues that the ``soldiers'' are the ones to be won over to new pursuasions about weaponry, which leads to the interesting conclusion that closer ties between academic researchers and DoD middle managers would be beneficial, rather than separation as now advocated by some academicians. I recommend that Risks Forum correspondents who wish to comment on weapons systems risks begin by reading WEAPONS AND HOPE before entering the debate. That way, some new ground might get covered.

Peter Denning

Re: <u>RISKS-1.34</u>, Wolves in the woods

Jim Horning <horning@decwrl.DEC.COM> 6 Jan 1986 1032-PST (Monday)

Dave,

I'm sure you meant "shooting at wolves" rather than "shooting at woods"?

Jim H.

Re: <u>RISKS-1.34</u>, Wolves in the woods

Dave Parnas <vax-populi!dparnas@nrl-css.arpa> Mon, 6 Jan 86 13:06:20 pst

I am glad that you are sure. I did mean wolves and not woods. I hope that everyone else is sure too. We aim for perfection but we don't do to vel.

Dave

Certifiable reliability and the purpose of SDI

<scott@rochester.arpa> Tue, 7 Jan 86 07:29:21 est

Jim McGrath's comments on reliability worry me quite a bit. He seems to understand, as do most of the technically literate, that there is no chance of protecting population centers with enough certainty to eliminate the Soviet incentive to own missiles. Yet this is precisely what the public thinks SDI is all about, and it is what our president proposed when he asked us to make nuclear weapons "impotent and obsolete."

At the risks forum at last month's ACM SOSP, someone pointed out that one of the most important responsibilities of a scientist or engineer is to MANAGE THE CUSTOMER'S EXPECTATIONS. It is both dishonest and EXTREMELY dangerous to proceed with SDI research if we and the public have fundamentally different understandings of the nature of that work.

It seems perfectly plausible to me that we could build space-based installations that would disable enough incoming missiles to, say, significantly increase the survivability of our own land-based defenses. Such installations seem to be the most likely product of SDI research. They may or may not be a good idea on strategic, economic, political, or social grounds. Any decision to proceed with their development should be preceded by public discussion and debate. Unfortunately, current debate is being focussed on the entirely different goal of omnipotent nuclear defense. We are marketing a product that we have no intention to deliver in order to build a product that we did not want to market.

Michael L. Scott, University of Rochester (716) 275-7745 scott@rochester.arpa {decvax, allegra, seismo, cmcl2}!rochester!scott scott%rochester@CSNET-RELAY

Putting a Man in the Loop

<scott@rochester.arpa> Tue, 7 Jan 86 07:03:08 est

I find it remarkable that this suggestion is taken seriously. Time scales simply do not permit it. As has been pointed out by previous contributors, human intervention during boost phase is out of the question, since it's all over in a minute or two. But even for later phases of missile flight, it is ridiculous to expect competent, cool-headed behavior from human operators who 1) have presumably been watching their consoles for years with no action, 2) have the fate of the world in their hands, and 3) have only a few minutes in which to make their decisions.

Michael L. Scott

🗡 Re: SDI Testing

Jim McGrath <J.JPM@LOTS-A> Mon 6 Jan 86 18:24:44-PST

From: horning@decwrl.DEC.COM (Jim Horning) Thanks for your comments. However, I do have to disagree with your cheerful assessment of the chances for REALISTIC testing of any SDI system or major subsystem. The problem is not that there is no testing that could be done, but that any substantial change in the system's environment is likely to provoke a new set of unexpected behaviors.... (Several very valid points are made about the difficulty of realistically testing SDI).

You are, of course, correct. The problem is that your points could also be (and are) made about any complex weapons systems (or indeed, any complex system at all). It is NEVER possible to fully test ANY system until it is actually used in battle (and even then it can fail in future battles). While the size of SDI makes some testing problems harder, others may be made easier. Specifically, SDI operates in a far more predictable environment that any earth based weapons system. Enemy countermeasures, so often cited as a problem, are a problem for ANY battle system, and once again the possible modes of response by the enemy need not be correlated to the size of the SDI system. Thus I would expect that a "realistic" (i.e. to a certain acceptable degree of reliability) testing of the Aegis carrier defense system to be as hard as testing SDI, even though the later is perhaps an order of magnitude smaller than the former. (note that software and system testing are not the same thing.)

My point was more that SDI (always excepting boost phase) could be tested according to the same type of standards we currently use to test other complex weapon systems (or computer systems, etc...). That is, the SDI testing problem is indeed a problem, but not one radically different from those that have already been encountered (and "solved"), or those likely to be encountered in the future. Thus attention should be focused on HOW to do the tests, not on decrying that the testing problem is somehow inherently impossible to solve.

Jim [McGrath, that is]

🗡 Re: Testing SDI

Jim McGrath <J.JPM@LOTS-A> Mon 6 Jan 86 18:40:51-PST

From: vax-populi!dparnas@nrl-css.arpa (Dave Parnas) The comments that you reported on testing SDI, proposing that we test it by shooting at periodic meteor swarms make me wonder how many of the people in our profession have trouble discriminating between real problems and arcade games. Shooting at an easily predictable non-evasive meteor has about the same relation to the real job of SDI as shooting at a target in a booth at a county fair has to shooting at woods in heavy brush from a moving airplane.

It is fairly obvious that Professor Parnes did not read my original message, nor the follow up messages. The original message dwelt on the COST of testing, and used meteor swarms as a simple example, not a serious proposal for exhaustive testing (as was clear in the context of the message). Indeed, I specifically stated that the example given would be good primarily for a basic test of tracking and "hard kill" capability.

Moreover, in more recent contributions I made clear that my central point is that testing of SDI is not somehow impossible, if you accept that we can test such systems as Aegis. Particularly, I think it incredibly naive to equate size of code with system complexity. (see my previous message on this). Now, one can dispute that such systems as Aegis are testable. Or one can hold SDI to higher reliability standards than systems such as Aegis. Both are defendable positions. But the first removes SDI from some unique class, and the second is quite debatable (depending upon your mission definition for each system).

Jim

🗡 Re: SDI Testing

Jim Horning <horning@decwrl.DEC.COM> 6 Jan 1986 1911-PST (Monday)

Jim,

If you think that I consider that the kind of testing that is done for present weapons systems is acceptable for a system of the importance, power, and risks of SDI, then we have been failing to communicate at a very fundamental level.

The kind of risk that is acceptable for the loss of an aircraft carrier and for the loss of all of human civilation are many orders of magnitude apart. The complexity of SDI and Aegis (and hence the difficulty of adequate testing) are many orders of magnitude apart. And the military hasn't done so well at testing in the past (DIVAD, Bradley Fighting Vehicle, plus the examples you cite) that I am willing to trust them to decide what testing would suffice here.

I do not consider arcade games to be a suitable model for this excercise.

Jim H.

M Dec. IEEE TSE: Special Issue on Software Reliability--Part I

Jim Horning <horning@decwrl.DEC.COM> 6 Jan 1986 1903-PST (Monday)

[This note is primarily for that small fraction of Risks that may not be regular readers of IEEE Transactions on Software Engineering. --Jim H.]

The December 1985 issue of TSE is devoted to software reliability. As has been noted many times in this forum, unreliable software is one of the principal sources of risks from computer systems.

A few things that caught my eye in this issue:

"The occurrence of major software failures is strongly correlated with the type and level of workload prior to the occurrence of a failure. This indicates that software reliability models cannot be considered representative unless the system workload environment is taken into account. The effect of workload on software reliability is highly nonlinear; i.e., there is a threshold beyond which the software reliability rapidly deteriorates. ... Although we may intuitively expect to find a higher software error rate with higher workload (partly attributable to greater execution), there appears to be no fundamental reason why both software and hardware should exhibit a similar nonlinear increase in the load-hazard with increasing workload."

"Recognizing the problem is only the first step; knowing what to do to achieve high confidence software still remains elusive. This is especially true in the area of software reliability, one of the prime factors affecting confidence (or lack of it) in software systems. Current DOD development programs are unable to achieve satisfactory software reliability in a consistent fashion because of the lack of understanding of what conditions truly affect reliability. This situation is compounded when you consider that software reliability requirements for future DOD systems will be much higher as functional demands on the software become more complex, as criticality of the software increases and as system components become more distributed."

"Abstract--When a new computer software package is developed and all obvious erros [sic] removed, a testing procedure is often put into effect to eliminate the remaining errors in the package."

"Successful Missions ... Proportion of fault-tolerant runs which completed without failing: 56 percent; Proportion of nonfault-tolerant runs which completed without failing: 47 percent."

"An intensity function, called the intensity of coincident errors, has a central role in this analysis. This function describes the propensity of programmers to introduce design faults in such a way that software components fail together when executing in the application environment. ... We study some differences between the coincident errors model ... and the model that assumes independent failures of component verions [sic].

"Certain intensity functions can result in an N-version system, on average, being more prone to failure than a single software component. ... The effects of coincident errors, as a minimum, required an increase in the number of software components greater than would be predicted by calculations using the combinatorial method which assumes independence. ... It is clear we need empirical data to truly assess the effects of these errors on highly reliable software systems."

🗡 Re: Masquerading

"R. Michael Tague" <Tague@HIS-PHOENIX-MULTICS.ARPA> Mon, 6 Jan 86 11:39 MST

In Risks Volume 1 Issue 34 it was suggested that a "trusted path" could be implemented by having trusted terminal driver software recognize "a combination of keystrokes from the user that would be defined to mean 'enter trusted path'." I would like to suggest that if one were to implement such a mechanism that one should make the "enter trusted path" signal be a single keystroke, i.e., one character or the out-of-band BREAK/ATTENTION key signal, not a "combination of keystrokes".

The reason is that it would be relatively easy for a malicious program to interfere with a multi-character signal. For example: most terminals can be made to send an answerback string to the host, a program that is trying to not be defeated by an "enter trusted path" signal could be constantly be sending answerback requests to the terminal. The terminal device driver would then not be able to recognize the combination of keystrokes that make up the "enter trusted path" signal due to the interleaving of answerback messages.

I suggest to anyone implementing such a trusted path mechanism that they use the out-of-band BREAK/ATTENTION key signal for the "enter trusted path" signal so that the user and applications will still have the full character set to work with. Whatever character/signal is used one should not be able to change or disable it.

Tague@CISL



Search RISKS using swish-e

Report problems with the web pages to the maintainer



Nancy Leveson <<u>nancy@ICSD.UCI.EDU</u>> 07 Jan 86 19:54:29 PST (Tue)

With regard to the note by Jim Horning about the special issue of IEEE TSE on Software Engineering - Part 1. He cites the following:

"An intensity function, called the intensity of coincident errors, has a central role in this analysis. This function describes the propensity of programmers to introduce design faults in such a way that software components fail together when executing in the application environment. ... We study some differences between the coincident errors model ... and the model that assumes independent failures of component verions [sic].

"Certain intensity functions can result in an N-version system, on average, being more prone to failure than a single software component. ... The effects of coincident errors, as a minimum, required an increase in the number of software components greater than would be predicted by calculations using the combinatorial method which assumes independence. ... It is clear we need empirical data to truly assess the effects of these errors on highly reliable software systems." Jim, in the next issue of TSE (part 2 of the special issue on software reliability) my paper with John Knight appears in which we describe our experiment (involving 27 programmers and two universities) which provides some of this empirical data. We found that independently produced software showed much higher coincident failures than would be expected assuming statistical independence. In later papers which have looked at the actual bugs (faults) in the software which was produced in the experiment, we found that people tended to make very similar mistakes or, at the least, to make mistakes on the same hard parts of the problem which lead to the programs failing on the same input data. In summary, our data supports the use of the coincident errors model rather than the independent failures model. The first paper on this will appear in February, two others are still in preparation or review.

All experimental evidence that I have seen to date does not support the conclusion that software with ultra-high reliability can be achieved by producing independent versions and voting the results although some reliability improvement may be possible. The question is whether enough is gained to justify the enormous added cost. Or whether the money and resources could better be spent in other ways.

We are just about to start another experiment which will attempt to get some data on whether people are able to write self-test statements (acceptance tests, assertions, exceptional conditions) which will detect errors at execution time. We will then be able to compare this type of fault detection with voting.

Nancy Leveson University of California, Irvine

🗡 SDI Testing

Nancy Leveson <<u>nancy@ICSD.UCI.EDU</u>> 07 Jan 86 20:19:06 PST (Tue)

>From: Jim McGrath <J.JPM@LOTS-A>
>I would expect that a "realistic" (i.e. to a certain acceptable degree
>of reliability) testing of the Aegis carrier defense system to be as
>hard as testing SDI, even though the later is perhaps an order of
>magnitude smaller than the former. (note that software and system
>testing are not the same thing.)

After speaking to some of the people working on Aegis, I would not use that as an example of a reliable system. I have heard that Aegis is anything but reliable. What is your source that shows it is highly reliable?

You seem to imply that because we have a system and it has been tested that it is reliable. Unfortunately, my experience has not supported this hypothesis. There are some that have argued that our current ABM and early warning systems are so complex that there is very little chance that they will ever work if so called upon. For example, in "Normal Accidents: Living With High Risk Technology" by Charles Perrow, he states about our current launch-on-warning systems:

"...if there were a true warning that the Russian missiles were coming, it looks as if it would be nearly impossible for there to be an intended launch, so complex and prone to failure is this system. It is an interesting case to reflect upon: at some point does the complexity of a system and its coupling become so enormous that a system no longer exists? Since our ballistic weapons system has never been called upon to perform (it cannot even be tested), we cannot be sure that it really constitutes a viable system. It just may collapse in confusion!" [Perrow, pg. 257-258]

It does not seem to be a very convincing argument that SDI can be tested by citing other systems which have been tested but never used enough to measure their reliability. How do we know how effective that testing has been? If you could give me a system which exists, is equivalent, AND has been in use enough to have good information on its reliability, then I would have to listen to you.

>My point was more that SDI (always excepting boost phase) could be >tested according to the same type of standards we currently use to >test other complex weapon systems (or computer systems, etc...). That >is, the SDI testing problem is indeed a problem, but not one radically >different from those that have already been encountered (and >"solved"), or those likely to be encountered in the future.

If you have information on the solution to the testing (i.e. software reliability) problem, please tell me. I could make a fortune because no one I know of seems to know that it has been solved or knows the solution. I have been involved in research in the area of software reliability and safety for many years because I thought it was an unsolved problem. Could you provide some references to the solution? (I will split my first million dollars in consulting fees with you.)

>Moreover, in more recent contributions I made clear that my central >point is that testing of SDI is not somehow impossible, if you accept >that we can test such systems as Aegis. Particularly, I think it >incredibly naive to equate size of code with system complexity. (see >my previous message on this).

Of course you can test any system. That is not the point. The question is whether the testing is complete and effective. For that, we need to know not whether Aegis was tested, but what is the reliability of Aegis.

>Now, one can dispute that such systems as Aegis are testable. Or one >can hold SDI to higher reliability standards than systems such as >Aegis. Both are defendable positions. But the first removes SDI from >some unique class, and the second is quite debatable (depending upon >your mission definition for each system).

I can believe that Aegis is not testable without removing SDI from the unique class. I don't understand your logic -- one has nothing to do with the other. No one is arguing that SDI is unique solely because it is untestable. Most complex software systems can not be made ultra-reliable using our current technology and, more important, there is no known way

to verify or measure that these systems are ultra-reliable even if they are. That does not mean that they do not involve unique problems or that they are of equal difficulty to build. They may all have different reliability -- but none of them can be proven to be ultra-reliable.

Moreover, I am not concerned about holding SDI to higher reliability standards than systems such as Aegis or others. I am concerned about just meeting those standards. My work is in the area of safety-critical systems where reliability requirements range from 10^(-5) to 10^(-9). There exist no current software technologies which will guarantee that the software meets these requirements or can be used to accurately measure software reliability in this range.

Nancy Leveson University of California, Irvine

🗡 SDI Testing

Dave Parnas <<u>vax-populi!dparnas@nrl-css.arpa</u> > Tue, 7 Jan 86 17:40:32 pst

I regret that I gave Jim McGrath the impression that I had not read his many submissions to RISKS before I responded to his suggestion that meteors could be used to test SDI-like systems. I wish to assure him that I had read them twice.

Given the importance of discrimination between legitimate warheads and decoys in a "Star Wars" battle, I would consider the defensive system to have failed if it fired at meteors. The capability to shoot down meteors could be considered, by normal engineering standards, an overdesign as well.

It is a mistake to consider "testable" as a predicate. Some systems are easy to test, others are hard to test. Systems like Aegis are difficult to test, but SDI would be more difficult. Further, the SDI requirements are stricter.

Multiple redundancy

<<u>ihnp4!utzoo!henry@ucbvax.berkeley.edu</u>> Thu, 9 Jan 86 12:14:34 PST

Advocates of multiple redundancy through independently-written software doing the same job might be interested in an incident involving complete failure of such a scheme.

During the development of the De Havilland Victor jet bomber, roughly a contemporary of the B-52, the designers were concerned about possible problems with the unusual tailplane design. They were particularly worried about "flutter" -- a positive feedback loop between slightly-flexible structures and the airflow around them, dangerous when the frequency of the

resulting oscillation matches a resonant frequency of the structure. So they tested for tailplane flutter very carefully:

1. A specially-built wind-tunnel model was used to investigate the flutter behavior. (Because one cannot scale down the fluid properties of the atmosphere, a simple scale model of the aircraft isn't good enough to check on subtle problems -- the model must be carefully built to answer a specific question.)

2. Resonance tests were run on the first prototype before it flew, with the results cranked into aerodynamic equations.

3. Early flight tests included some tests whose results could be extrapolated to reveal flutter behavior. (Flutter is sensitive to speed, so low-speed tests could be run safely.)

All three methods produced similar answers, agreeing that there was no flutter problem in the tailplane at any speed the aircraft could reach.

Somewhat later, when the first prototype was doing high-speed low-altitude passes over an airbase for instrument calibration, the tailplane broke off. The aircraft crashed instantly, killing the entire crew. A long investigation finally discovered what happened:

1. The stiffness of a crucial part in the wind-tunnel flutter model was wrong.

2. One term in the aerodynamic equations had been put in wrongly.

3. The flight-test results involved some tricky problems of data interpretation, and the engineers had been misled.

And by sheer bad luck, all three wrong answers were roughly the same number.

Reference: Bill Gunston, "Bombers of the West", Ian Allen 1977(?).

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

Reply to Dr. Denning on Freeman Dyson

Gary Chapman <<u>PARC-CSLI!chapman@glacier</u>> Tue, 7 Jan 86 18:07:26 pst

To: glacier!RISKS@SRI-CSL.ARPA

I have considered Dr. Peter Denning's thoughts on strategic defense with some care, and I have appreciated the thought he has put into the issue. I also have a great deal of respect for Freeman Dyson, whose book, Weapons and Hope, Dr. Denning recommended we all read, and particularly those of connected with the policies of CPSR. I would like to respond to some of those comments. First, the concept of an anti-ballistic missile defense in a "non-nuclear" world is contradictory. If nuclear weapons and ICBMs have been eliminated, there is no need for an ABM system with all its expense and uncertainties. Dr. Dyson says in his book that he favors a strategic defense only after a radical cut in offensive nuclear weapons on both sides. Very few critics of the SDI would quarrel with this, including me. But we are so far from the kind of cuts that Dr. Dyson and Dr. Sidney Drell, who also favors this goal, feel are required before strategic defense is considered that it is hardly worth considering at all at this point. It is particularly dangerous to consider upsetting the strategic balance by developing and deploying a strategic defense before those cuts are made.

What CPSR has said is that the software problems inherent in the development of an SDI-type ABM battle management system contribute to strategic instability, and therefore the deployment of the SDI will leave us worse off than without it. An ABM system that is deployed AFTER achievement of substantial and trustworthy strategic stability would not have the same mission as the SDI. It would be an added insurance of a stability already achieved by other means, it would be a safeguard against ICBM accidents and against third-party powers. It would not be a radical change in the strategic balance the way the SDI would be if it were to be deployed in the current strategic situation.

Despite the good will of the President and his honorable intentions, the SDI is clearly a war-fighting program. I have never gotten the impression from Dr. Dyson that he is in favor of such an effort. CPSR has opposed the SDI for the program that it is, not for the program that it could be.

Gary Chapman Executive Director, CPSR

Peter Denning on WEAPONS AND HOPE

Jon Jacky <<u>jon@uw-june.arpa</u> > Wed, 8 Jan 86 20:56:23 PST

> (Peter Denning writes:)

> ...CPSR has issued position statements against SDI based on the premise that> SDI is nothing more than an ABM system...

I think the point of those statements was that systems with limited capabilities, such as defense of hardened missile silos, fall far short of the sort of comprehensive defense implied by the SDI's stated goal of "eliminating the threat posed by nuclear ballistic missiles."

> Dyson argues that the 'soldiers' are the ones to be won over to new> pursuasions about weaponry, which leads to the interesting conclusion

- > that closer ties between academic researchers and DoD middle managers
- > would be beneficial, rather than separation as now advocated by some

> academicians.

I am not aware of any academicians who say that soldiers and scholars should



Mike McLaughlin <<u>mikemcl@nrl-csr</u> > Wed, 8 Jan 86 05:48:49 est

I note with dismay the ad-hominem phraseology that is appearing in the SDI discussions. It is understandable but unacceptable. The issue is too important. I request that the participants review their inputs prior to submission, and edit out phraseology that is not relevant to the issue. It is not fair to expect the forum's moderator to be a censor. - Mike McLaughlin [Thanks. PGN]

[I have received various complaints about some of the recent SDI verbiage -- its quality, accuracy, relevance to RISKS, what right has RISKS to distribute SRI discussion when it should be in ARMS-D, etc. In general, I have to hope that our contributors exert some good sense. Some of the nit-picking should clearly be resolved privately. In some cases I might request two antagonists get together and write a single position statement to which they both agree -- but that seldom works.

So, at this point I would like to elevate the quality of SDI discussion -- but not to stifle meaningful discussion that is really

RISKS-related. SDI remains one of the most important issues confronting us, and open

✓ Testing: Differences between SDI and other systems.

<<u>Karl.Kluge@G.CS.CMU.EDU</u>> 7 Jan 1986 22:41-EST

Message-Id: <505539701/kck@G.CS.CMU.EDU>

> Date: Mon 6 Jan 86 18:24:44-PST

> From: Jim McGrath <J.JPM@LOTS-A>

>

> You are, of course, correct. The problem is that your points could
> also be (and are) made about any complex weapons systems (or indeed,
> any complex system at all). It is NEVER possible to fully test ANY
> system until it is actually used in battle (and even then it can fail
> in future battles).

- The consequences of failure of an SDI system are orders of magnitude greater than the consequences of failure of a "normal" weapons system. We damn well should be orders of magnitude more confident in it.
- 2) Which is really irrelevant, since the function of the SDI is to enhance deterrence, not replace it. The SDI system doesn't have to work, it just has to create reasonable worry that it might work in the mind of a potential attacker. This makes it different from most systems, which are built to be used. If the SDI system ever has to be used then it has failed, which means...

(* rest of message on ARMS-D. Karl *) [THANKS... PGN]

My opinion, of course, in no way reflects the opinion of anyone I'm associated with. Karl

Testing SDI

Robert Goldman <<u>rpg%brown.csnet@CSNET-RELAY.ARPA</u>> 8 Jan 86 (Wed) 15:26:18 EST

In <u>RISKS-1.34</u> Jim McGrath discusses testing the SDI. A common objection to the SDI is that it could not realistically be tested.

McGrath correctly points out that this is true of any modern weapon system. I agree with this basic point, but of course, some weapons systems are easier to test than others. For example, Mr. McGrath points out

it took WWI for the Germans to realize that the lessons of the 1880's concerning rapid infantry fire (and thus the rise of infantry over calvary) did not take artillery development adequately into account

This is correct, but dodges the point that at that time, modern artillery,

rifles and machine guns HAD all been fired in anger. The almost universal inability to profit from the experience was due to institutional failures, rather than lack of raw data.

I need hardly point out that ICBMs and SLBMs have NOT been tested in wartime conditions, and that we have reason to believe that there won't be a second chance to correct any mistakes.

Mr. McGrath goes on to suggest that the SDI might be tested against meteor storms. I question this for three reasons:

1. As I understand it, the particle-beam weapons of the SDI are not intended to destroy warheads outright, but rather prevent them from reaching their targets and detonating. How would one judge that a meteorite's fusing and guidance mechanisms had been destroyed?

2. Meteorites are not human-made objects which are designed with an eye to penetrating enemy defenses: they do not drop chaff, employ electronic counter-measures, etc.

3. Meteorites have a wholly different flight pattern. As I understand it, ICBMs have a boost phase, a cruising phase and a re-entry phase. Doesn't a missile's detectability and vulnerability depend on which of these phases it is in?

Robert Goldman

[I deleted a paragraph on what might happen "if the SDI accidentally (or on purpose) shot down a Soviet reconnaissance satellite?" PGN]

Summing Up on SDI

Jim McGrath <<u>J.JPM@Epic</u>> Thu 9 Jan 86 22:45:57-PST

To: "risks@sri-csl"@Sushi Reply-to: mcgrath%mit-oz@mit-mc.arpa

> [Reminder: I have omitted a bunch of McGrath-Lin messages. If you wish to read them, see aove. PGN]

From all these messages, I've come to two conclusions. First, that on the whole, I tend to feel that SDI is a more complex system (mainly because of its mission size) than existing ones, such as Aegis. But I could be wrong (either way). And I do not believe that it is "orders of magnitude" more complex than existing systems. Thus it would seem that it could be built to existing system performance standards.

The second question is whether these standards are "adequate," and if not can we improve upon them? It is clear that existing systems are not being tested as fully as possible (Herb Lin's report on the Aegis tests makes them appear to be a joke). I've already pointed out that substantial testing of mid-course and terminal phases, far more extensive testing than any of our other systems have received, can be carried out. Thus, provided we have a proper commitment, even our current testing technology can be better applied (with better results) than we have done up until now.

To a large extent the standard you require depends upon your definition of the mission of the system. Clearly the system was never designed to make OUR nuclear weapons obsolete (just the Soviet's). So under any mission we would probably retain a force sufficient to destroy the USSR, and so can always fall back on MAD. Any reasonable performance level would protect our weapons to a significant extent (and if not, you can always keep a sub force). So the real question is whether it can protect cities.

I would tend to doubt it, under a full and unimpeded Soviet attack. But there are many scenarios (from accidental launch to a limited (decapitation or counterforce) strike to a second strike (the first perhaps going to Europe and/or China)) where it quite possibly could.

In any event, I am certainly not sure enough to either commit to SDI deployment nor to terminate research. Since all SDI is at the moment is research, I have no problem with the existing program. Still, knowing how programs have a tendency to outlive their usefulness, I think strong scrutiny is appropriate. But not mindless opposition.

Jim



Search RISKS using swish-e

Report problems with the web pages to the maintainer



Dave Wade <<u>djw%a@LANL.ARPA</u> > Fri, 10 Jan 86 14:38:54 mst

I am just a programmer; however, for three and a half years I worked at CTR Division here at Los Alamos. I augmented (in a very minor way,) and maintained the control system for a series of Magnetic Fusion Energy experiments.

The programs ran in "real time" and attempted to use magnets to "contain" and shape a plasma. The plasma is very like the ball of gas in your neon light over your desk, but instead of neon, we used a vacuum and a tiny amount of sulfur-hex... (that same stuff that was in the tank in Oklahoma that the workmen dropped because it was overfull). The plasma is started by discharging a huge arc across a quartz bottle that contains the vacuum and the sulphur-hex. The computer controls the point at which huge capacitors discharge through the quartz bottle. There are many independent power supplies that discharge through different portions of the quartz bottle. The computer program controls "precisely" when each power supply or capacitor bank discharges into the quartz tube. These power supplies/ capacitor banks are placed by the physicists such that the ball of lightning (plasma) formed inside the quartz tube is kept from touching the inside of the tube. The power supplies form a magnetic bottle inside the guartz tube (the guartz tube is about 14 inches across,) and under computer control have kept the plasma alive and away from the edge of the

14 inch wide tube for more that 3/100 ths of a second. Now the tube has been made about twenty feet long and the ball of plasma has been created, stabilized, and then slowly (different time frame) moved to the other end of the tube; controlled by a Pr1me 300 (I'd guess that is about the same as any of the 68000-based micros). The Pr1me did all of this stuff remotely over a fiber-optic CAMAC highway.

The point of this was that any failure of the control system was capable of killing personnel. The "man in the loop" who was running the control system was not necessarily knowledgeable about what he was controlling (sometimes this was me...). The software was much smarter than the operator and certainly swifter. There is no way that I could hit the "kill" switch before the plasma got loose. The "kill" switch was used as a mechanical lockout (in conjunction with the software lockout and the "key switch" we had installed) while we were testing the control system.

I sit here and am bored by endless arguments on Unix "news" that the Strategic Defense Initiative contains portions which "can't be programmed" because they have this or that seemingly insurmountable characteristic. I look at my friends MacIntosh and think fondly of the days when I helped with the payroll and accounting for a 2000 person company on an IBM 1411 which wasn't the machine that the Mac is... What may be "impossible" for me is resting forgotten in one of the software libraries down the hall.

🗡 Big Brother

Jim McGrath <<u>J.JPM@Epic</u>> Wed 8 Jan 86 19:53:41-PST

To: "risks@sri-csl"@Sushi Reply-to: mcgrath%mit-oz@mit-mc.arpa

Has anyone noticed the proposals made in the article "Security Without Identification: Transaction Systems to Make Big Brother Obsolete" by David Chaum in the October issue of Communications of the ACM (vol 28, # 10, 10330-1044)? If so, what is the response? Basically, he asserts that it would be in the interests of both individuals and organizations to adopt a system whereby transactions would be essentially unforgeable and untraceable.

Jim

🗡 Re: Big Brother

Peter G. Neumann <<u>Neumann@SRI-CSL.ARPA</u>> Thu 9 Jan 86 21:34:07-PST

To: mcgrath%mit-oz@MIT-MC.ARPA

What you suggest might indeed be an improvement. However, remember that

nothing is guaranteed unforgeable. You will always have some points of vulnerability, and you have risks of spoofing, clever system programmers, embedded Trojan horses in hardware and software, etc.

If you were to rely blindly on such a system, you would be making yourself even more vulnerable! You can indeed come closer to having an unforgeable communication, but believing that you have it may actually increase the risk.

Peter

Men in the SDI loop

Herb Lin <<u>LIN@MC.LCS.MIT.EDU</u>> Sat, 11 Jan 86 17:54:43 EST

To: mooremj@EGLIN-VAX.ARPA cc: LIN@MC.LCS.MIT.EDU, risks@SRI-CSL.ARPA

- > As has been pointed out by previous contributors, human intervention during
- > boost phase is out of the question, since it's all over in a minute or two.

From: mooremj@eglin-vax

For SLBMs, or missiles aimed at Europe from the western Soviet Union, I'll grant the point. But for land-launched missiles aimed at the US, I estimate at least a five-minute boost. If this is wrong, someone please correct me!

Currently, the SS-18 has boost phase of about 5 minutes = 300 sec. MX has a boost phase of 180 sec. Probably 120 sec boost isn't impossible if you really tried to do it (as the Sovs will undoubtedly do if we ever deploy SDI). Indeed, the US is studying fast burn boosters even as I write this.



Search RISKS using swish-e

Report problems with the web pages to the maintainer


Jim Ziobro <<u>rocksvax!z@rochester.arpa</u> > Fri, 17 Jan 86 13:39:48 est

I believe the point of Chaum's article was to show how computer technology might prevent invasions of privacy by unauthorized parties. He did not give specific algorithms. The challenge is now to develop secure algorithms and to get public acceptance. All in all I thought it was a very good article.

As PGN points out, a completely secure algorithm is impossible. But all we really need do is get one that is better than our current coupon system. How secure is our coupon system (Dollars and coins)? Well at least one person in Xerox can make money (given the proper paper) that will fool most of the population. A friend in printing says that passable money is quite easy to do but this particular individual had better things to do with his time.

The privacy of currency is hard to beat. But already many people prefer credit cards to the vulnerability of cash. In that case they trade off security for allowing nearly anyone at their bank to see where they shop and how much they spend. People are also willing to spend the \$20/year for the credentials/security that credit cards offer.

I think public acceptance increases by one everytime someone receives a false transaction on their credit card or even when their Social Security

check is stolen in the mail. At that rate Chaum's vision of the future may be with us before 2000.

//Z\\ James M. Ziobro Ziobro.Henr@Xerox.ARPA {rochester,amd,sunybcs,ihnp4}!rocksvax!z

🗡 Big Brother

"Keith F. Lynch" <<u>KFL@MC.LCS.MIT.EDU</u>> Mon, 13 Jan 86 21:33:27 EST

To: mcgrath@OZ.AI.MIT.EDU cc: KFL@MC.LCS.MIT.EDU, <RISKS@SRI-CSL.ARPA

Date: Wed 8 Jan 86 19:53:41-PST From: Jim McGrath <J.JPM@Epic>

... David Chaum ... asserts that it

would be in the interests of both individuals and organizations to adopt a system whereby transactions would be essentially unforgeable and untraceable.

I agree that this would be great. I doubt that it will happen. The character of people in government today is very different from 200 years ago. It is obvious that the signers of the constitution would have extended their protections of papers and places to computer files and disks, had they heard of such things. Confiscation of CBBS computers is just as wrong as confiscation of printing presses. 'Fairness' rules concerning radio and TV are just as unreasonable as similar rules concerning newspapers and magazines would be. The only reason why the printed media get preferred treatment is that they were explicitly mentioned in the constitution. Had radio, TV, electronic funds transfer systems, and telephones been around in the days of Jefferson and Washington, I am sure that they would enjoy similar constitutional protection.

There are many good reasons why it is in the government's interest to be able to track each individual's finances, phone usage, electronic mail usage, etc. Mainly to fight crime, especially the new bugaboo of terrorism. But this same reasoning could have been used by the writers of the constitution, but it wasn't. It was believed that the benefits of having a free society outweighed the problems of some people abusing these freedoms. Two hundred years later, comparing our country with countries that made the opposite decision, I think we did the right thing.

I believe that this is probably the greatest risk of computers. That by phasing out the media that are mentioned in the constitution, that we are also phasing out the protections long enjoyed by their users.

...Keith

Re: Multiple redundancy

<<u>ihnp4!utzoo!henry@ucbvax.berkeley.edu</u>> Mon, 13 Jan 86 19:49:18 PST

A correction and an addendum to my earlier contribution about multiple redundancy...

Correction: It was not the "De Havilland Victor" but the "Handley Page Victor". Blush. That's like calling Boeing "McDonnell Douglas".

Addendum: The full reference is Bill Gunston, "Bombers of the West", Ian Allan, London 1973, page 92.

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

COMPASS 86 Call for Papers

Al Friend <<u>friend@nrl-csr</u> > Tue, 14 Jan 86 10:19:26 est

> COMPUTER ASSURANCE System Integrity: Process Security and Safety

Important DatesDate & Location------------March 31, 1986July 7 - 11, 19863 Copies of Abstract SubmittedThe George Washington University

April 30, 1986Washington, D.C.Authors Notified of AcceptanceAccomodations available in Dorms

May 30, 1986 Camera Ready Manuscripts Due

Keynote Address by: David Lorge Parnas

Sponsored by: WASHINGTON SECTION IEEE Conference Name: COMPASS 86 (COMPuter ASSurance)

Our safety, health and welfare as individuals and as a nation are increasingly dependent on the correct use of computers. However it is usual to find major "bugs" and untrustworthy operation in critical computer controlled systems, despite advances in software engineering and computer system design. New approaches are needed. The purpose of this conference is to discuss these

Subject Areas Include (but are not limited to): X For information contact: X Subject Areas Include (but are not limited to): X For information contact: X Subject Areas Include (but are not limited to): X For information contact: X X COMPASS, P.O. Box 3815 X COMPASS, P.O. Box 3815 Specifications X Gaithersburg, MD 20878 Y Gaithersburg, MD 20878 Y Frocesses X friend@nrl-csr Y Assessment and Measurement X Y Formal methods and tests X Affiliation X Y Human limitations X Address X Y Kernels X City, State, Zip X X X Lisubmissions reviewed by program committee		*****
X Albert W. Friend, Prog. ChmnX X COMPASS, P.O. Box 3815 Specifications X Gaithersburg, MD 20878 Processes X friend@nrl-csr X Assessment and Measurement X NAMEX Formal methods and tests X AffiliationX Human limitations X AddressX Kernels X City, State, ZipX All submissions reviewed by program committee	Subject Areas Include (bu	t are not limited to): X For information contact: X
X COMPASS, P.O. Box 3815 X Specifications X Gaithersburg, MD 20878 X Processes X friend@nrl-csr X Assessment and Measurement X X Formal methods and tests X NAMEX Human limitations X AffiliationX Implementations X AddressX Kernels X City, State, ZipX JI submissions reviewed by program committee XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX		X Albert W. Friend, Prog. ChmnX
* Specifications X Gaithersburg, MD 20878 X * Processes X friend@nrl-csr X * Assessment and Measurement X X * Formal methods and tests X NAMEX * Human limitations X AffiliationX * Implementations X AddressX * Kernels X City, State, ZipX X X X JI submissions reviewed by program committee XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX		X COMPASS, P.O. Box 3815 X
* Processes X friend@nrl-csr X * Assessment and Measurement X X * Formal methods and tests X NAMEX * Human limitations X AffiliationX * Implementations X AddressX * Kernels X City, State, ZipX X X X	* Specifications	X Gaithersburg, MD 20878 X
* Assessment and Measurement X X * Formal methods and tests X * Formal methods and tests X * Human limitations X * Implementations X X Address * Kernels X X City, State, Zip X X	* Processes	X friend@nrl-csr X
⁴ Formal methods and tests X NAMEX ⁴ Human limitations X AffiliationX ⁴ Implementations X AddressX ⁴ Kernels X City, State, ZipX X Ul submissions reviewed by program committee XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX	* Assessment and Measur	rement X X
* Human limitations X AffiliationX * Implementations X AddressX * Kernels X City, State, ZipX XX XX	* Formal methods and tes	sts X NAMEX
^c Implementations X AddressX ^c Kernels X City, State, ZipX XX XX All submissions reviewed by program committee XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX	* Human limitations	X AffiliationX
<pre>* Kernels X City, State, Zip X X X </pre>	* Implementations	X AddressX
XX	* Kernels	X City, State, ZipX
VII submissions reviewed by program committee XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX		XX
	All submissions reviewed	by program committee XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
Search RISKS using swish-e		Search RISKS using <u>swish-e</u>



Peter G. Neumann <<u>Neumann@SRI-CSL.ARPA</u>> Sun 19 Jan 86 16:29:27-PST

To: RISKS@SRI-CSL.ARPA

This issue of RISKS once again concerns the topic of SDI, both in its own right and as being illustrative of a collection of risks from which we can learn for other applications. The problems that arise in considering SDI are some of the most fundamental problems affecting our lives at the moment. The news item that follows this message was probably seen by most of you who read newspapers. It is included here for the record, and for any of you who missed it.

Occasionally I get a complaint that the RISKS Forum seems biased. Some of those comments have come from proponents of SDI. I continually seek to include both sides of any critical issue. If only one side is willing to speak out, RISKS may appear biased to those who do not want to get drawn into the discussion. That is unfortunate, particularly if one side can eschew debate and then complain that the debate is rigged. Oh, well, we are damned if we do, and damned if we don't. Our ACM sponsorship stated at the outset of this Forum that we should make every attempt to be nonpartisan. I have on various occasions offered RISKS as an outlet to the SDI panel, but have been rebuffed with "RISKS is biased". Too bad. It looks as if some serious though went into the report that is described below, and it should certainly have the benefit of exposure to the social process. But if the proponents of SDI are hiding under a protective shield other than the one

they are trying to create, then that is an anti-social process instead.

As I have noted earlier, it is certainly easier to criticize others than to offer alternatives. Generally, the proof of the pudding is in the eating. Since the pudding has not jelled yet (indeed, it has not been cooked, which is fortunate in that suitable recipes do not yet exist), discussion is based on such things as dietary customs, a liking for untasted goodies, bad experiences with the effects of overly rich food, or allergy to pudding. De gustibus non disputandem est.

It is significant that software problems are explicitly identified in the cited report as being critical to SDI. (That conclusion was certainly self-evident a priori, but its being emphasized will certainly point to many problems that must be addressed -- not just for SDI). The risks therein are enormous, and I hope that RISKS will objectively discuss them (along with other risks) and what can be done to avoid them. SOFT-ENG should also have much valuable material on the techniques and role of software engineering.

However, as a meta-issue that is certainly relevant here, it is a tragedy of our times that software engineering techniques are still not widely used by the commercial developers of critical software. Some of those developers are literally many years behind the state of the art. The fault is probably distributed in many places, such as researchers who do not make their research and development tools really amenable to realistic use; software developers who take too many short-cuts and are too concerned with profits; government administrators who do not insist on higher-quality software with carefully preestablished requirements, and who do not follow through with strict control measures and penalties; politicians who create and perpetuate the bureaucracy; and the general public -- which puts up with it all. The waste is enormous -- not only in dollars, but in human resources and misplaced efforts. (I am referring here generically to a wide class of developments, not to SDI alone.)

Peter

✓ Unreleased SDIO Computing Panel Report

Walter Hamscher <<u>hamscher@MIT-HTVAX.ARPA</u>> Sat, 18 Jan 86 12:07:27 est

From the Boston Globe, page 1, Saturday, 18 Jan 1986

SPECIALISTS FAULT `STAR WARS' WORK

By Fred Kaplan Globe Staff

WASHINGTON - In a report commissioned by the Pentagon's Strategic Defense Initiative Office, a group of top computer software experts concludes that the SDI office is going about the task of building a `star wars' missile-defense system the wrong way.

The report does say developing a proper software program for SDI is feasible. However, it says the SDI office and its defense contractors are assuming they can develop the `star wars' weapons and sensors first and write its computer software afterward - when, in fact, an effective defense will be impossible unless this order is reversed.

The authors of the report, all avowed supporters of the SDI program, met for 17 days last summer and held further discussions before writing the report. The report was submitted to the SDI office last month, and has not been released publicly.

Software must be programmed to enable automatic communication between the satellites that detect Soviet missiles and the SDI weapons that will shoot the missiles down; between these weapons and other sensors that can distinguish missiles from decoys and assess whther the target was hit or missed; and between this entire network and political authorities on the ground. Hundreds of satellites, battle stations, sensors, giant space mirrors and other devices would be involved. Computations must be made, and orders must be given, in a matter of microseconds, with continuous updates and revisions.

The report says all the various designs for strategic defense systems proposed thus far demand "excessively sophisticated software" that "cannot be adequately tested." A design "that cannot be tested ... is of no value," the report says. And "excessively complex software cannot be produced at any cost."

John Pike of the Federation of American Scientists, a critic of SDI who did not serve on the panel that wrote the report, puts the problem this way: "It's like buying a home computer first and then discovering that the software you need won't run on it. Or it's like buying a Betamax and then discovering that your favorite movies are only on VHS.

"This report," Pike continues, "says a lot of the money in the [SDI] budget now is wasted because you'll end up buying the wrong machines."

The report emphasizes that computer software programming is still a young field with many unknown elements. The report states, "The panel expects no technological breakthrough that would make it possible to write the celebrated `10 million lines of error-free code,'" which SDI officials have acknowledged are necesary to make the system, as currently envisioned, work.

Moreover, "there are no laws or formulae that can accurately predict the successs or failure of a large software development." Nor is it possible today, the report says, to measure whether a software program can be applied to an SDI battle-management system.

The report says these problems are not impossible to solve. However, it says it will take at least two decades - and then only if the organization of the program is radically changed. Assuming these fundamental uncertainties can be resolved, the report cites other computer and software difficulties. Among them:

* Flights of the space shuttle have frequently been delayed because of computer problems found at the last moment. Yet whereas the shuttle's computers are designed to reain in operation for 1,000 hours without breaking down, the computers on board the satellites used in an SDI system would have to be built to break down only once every 100,000 hours.

David Parnas, a software specialist at the University of Victoria in British Columbia, also says the experience of several shuttle flights has allowed NASA to work out programming "bugs" over time. "This kind of thing couldn't possibly work with SDI," he says. "You can't call the Russians in the middle of a war and say, `Wait a minute, we have to recalculate some things.'"

Parnas was appointed a member of the panel that wrote the report. However, he resigned a few weeks after its formation, saying its work was pointless because SDI's software requirements were impossible to fulfill.

Stephen Berlin of MIT's Laboratory for Computer Sciences [sic], notes another difference between SDI and the shuttle: "The space shuttle is not being shot at. An SDI system almost certainly would be."

* The system would be highly vulnerable not only to direct attack but to nuclear weapons exploded in space as far as 1,000 kilometers away. "The high-energy neutron flux from a nuclear explosion is expected to `erase' volatile semiconductor memory," the report says. "Effective shielding is difficult."

The report recommends new ways of dealing with strategic defense that organize the various components of an SDI system in a "loose hierarchy," with tasks "delegated to and localized within parts of a system." Such a system would involve less complex and more testable software, and could be adapted more easily to change.

The authors of the report - all software specialists at top universities - acknowledge that it is not clear how to do all this, and that the SDI office should "use independent contractors" who could "tap the talent of leading researchers in the scientific community," to study the problem further.

Man in the loop and magnetic bottles

Jon Jacky <<u>jon@uw-june.arpa</u> > Sat, 18 Jan 86 16:37:24 PST

> (Dave Wade writes...)

> I ... maintained the control system for a series of Magnetic Fusion Energy
> experiments. The programs ran in "real time" and attempted to contain and
> shape a plasma. ... The point of this was that any failure of the control
> system was capable of killing personnel. ... The software was much smarter
> than the operator and certainly swifter. There was no way that I could
> hit the "kill" switch before the plasma got lose.

With all respect, I am having trouble accepting that there is not some misunderstanding or overdramatization in this account. Are we to believe that people stood around where they could have gotten killed if the control system failed? If this is true, the risks in question were certainly unnecessary. Why on earth were the operators not protected behind some kind of blast shield? What assurances did they require to convince themselves that the software was sufficiently bug-free that they could trust their lives with it?



Search RISKS using swish-e

Report problems with the web pages to the maintainer



Peter G. Neumann <<u>Neumann@SRI-CSL.ARPA</u>> Tue 28 Jan 86 09:45:12-PST

To: RISKS@SRI-CSL.ARPA

For those of you who haven't heard, the Challenger blew up this morning, 1 minute and 12 seconds after launch, during maximum thrust. Everything appeared to be working properly. TV pictures show one of the solid rocket boosters on the side going first, then everything. (There had been some concern because the temperature went below 28 degrees Fahrenheit during the night at Canaveral, and that temperature is considered critical because of ice formation.) The Challenger had consistently been the most reliable of all the shuttles.

One unvoiced concern from the RISKS point of view is the presence on each shuttle of a semi-automatic self-destruct mechanism. Hopefully that mechanism cannot be accidentally triggered.

When you start an engine at 40 below, you could be injured...

David Wade <<u>djw%f@LANL.ARPA</u> > Tue, 21 Jan 86 10:42:37 mst

I did not intentionally deceive you or overdramatize the risks taken during

checkout of "my" Fusion experiments. (I say "my" because I'm proud of them and they are the only ones I've ever worked on.)

People were normally behind blast walls during operation. However, certain individuals became familiar enough with the "normal" operation of the machine (and, at times, frustrated with certain types of idiosyncratic behavior) did put themselves at risk in order to trace down short circuits.

People became convinced (with time) that the software was reliable. Note that routine operation after "checkout" was complete was a lot different than operation during "checkout".

We normally operated behind blast walls with 2-3 video cameras (and finally got a vcr). One video camera was hung where it could "see" most of the power supplies. That camera had a zoom lense and it was routed through a "frame grabber" which was triggered off the master trigger. Many times that camera would "bloom" with the most dramatic evidence of a direct short.

Visitors see the remains of the capacitor which exploded years ago on the CTX experiment. The safety record is excellent, but it could be ruined at any time by stupidity.

None of the articles I've seen have criticised the SDI on the basis of the stupidity of the operators, so I wasn't "flaming" that point. I personally believe that the stupidity is evidenced by the lack of a world concensus for exploration of space and demilitarization of the world situation.

Perhaps this is just "liberal crap" left over from my youth in the 60's; perhaps I should re-examine my beliefs, but I think back on my life as an "Air Force Brat" whose father was in SAC (the Strategic Air Command) in the 50's, and I remember "the bay of pigs" week. That's probably one of the closest "near-death" experiences you've ever had, aren't you thankful that you made it? How did you feel? Did it hurt? Did you feel any different when you packed your sleeping bag and your tent in the station wagon and left for the mountains with the rest of the kids and moms that you knew? Do you think that people have that same feeling now when they discuss survivability?

I think that SDI has given the flower children their first hope since 1957. If it does only that, it has helped the world by forcing negotiations.

"Brazil" and Risks to the Public

Martin Minow, DECtalk Engineering ML3-1/U47 223-9922 <<u>minow%rex.DEC@decwrl.DEC.COM</u> > Monday, 20 Jan 1986 05:43:12-PST

Readers of the RISKS Forum might enjoy seeing the new movie, Brazil, which has been described as 1984 redone by Monty Python.

Martin Minow minow%rex.dec@decwrl.arpa





Keliability of Shuttle Destruct System [LONG]

"MARTIN J. MOORE" <mooremj@eglin-vax> 28 Jan 86 14:06:00 CDT

Copyright © 1986 Martin J. Moore [COMMENT: READERS -- PLEASE OBSERVE THE RESTRICTIONS ON THIS MESSAGE AT THE END OF THE MESSAGE. PGN]

> From: Peter G. Neumann <Neumann@SRI-CSL.ARPA>

> For those of you who haven't heard, the Challenger blew up this morning...

> One unvoiced concern from the RISKS point of view is the presence on each

> shuttle of a semi-automatic self-destruct mechanism. Hopefully that

> mechanism cannot be accidentally triggered. [COMMENT: I did not intend

to imply that as the cause -only to raise concern about the safety of such mechanisms. PGN]

Peter, I assume that you are talking about the Range Safety Command Destruct System, which is used to destroy errant missiles launched from Cape Canaveral. From 1980 to 1983 I was the lead programmer/analyst on the ground portions of that system, and I am the primary author of the software which translates the closing of destruct switches into the RF destruct signals sent to the vehicle. I think I can address the question of whether the system can be accidentally triggered; worrying about that gave me nightmares off and on for months while I was on the project. I'd like to tell you a little about the system and why I think the answer is No. Note that my information is now three years old, and some details may have changed; there may also be minor errors in detail due to lapses in my memory, which isn't as good as my computer's!

On board the vehicle, there are five destruct receivers: one on the external tank (ET) and two on each of the solid rocket boosters (SRBs). There is no receiver or destruct ordnance on the Orbiter; it is effectively just an airplane. The casing of each SRB is mined with HMX, a high explosive; the ET contains a small pyrotechnic device which causes its load of liquid hydrogen and liquid oxygen to combine and combust. The receivers and explosives are connected such that the receipt of four proper ARM sequences followed by a proper FIRE sequence by any of the receivers will explode the ordnance.

The ARM sequence and FIRE sequence must come from the ground; they cannot be generated aboard the vehicle. These sequences are transmitted on a frequency which is reserved, at all times, for this purpose and this purpose alone. There are several transmitters around the Eastern Test Range which can be used to transmit the codes. These transmitters have a power of 10 kw (continuous wave). The ARM and FIRE sequences consist of thirteen tone pairs (different for each command and changed for each launch). There are eight possible tones, resulting in 28 possible tone pairs; thus, there are (28^13) or slightly over 6.5E18 correct sequences.

The Range Safety Officer has two switches labeled "ARM" and "DESTRUCT". When he throws a switch, it generates an interrupt in the central processor (there are actually two central processors running and receiving all inputs, but only one is on-line at any time; in case of software or hardware error the backup is switched in. And yes, they have different power sources.) The central program checks for the correct code on each of two different hardware lines (the correct code is different for each line); if correct, and all criteria are met to allow the sequence to be sent, the central program requests the tone pairs for that sequence from another processor. That processor (like everything else in the system, actually redundant processors) has only one function: to store and deliver those tone pairs. The processor resides in a special vault and can only be accessed in order to program the tone pairs (which are highly classified) before each launch. The data line between the central processor and the storage processor is electrically connected ONLY when the ARM or DESTRUCT switch is actually thrown; this prevents a wild program from retrieving the tone pairs.

When the central program has retrieved the tone pairs, it formats a message to the currently selected remote transmitter. As the final step before sending the message, the program checks the switch hardware one more time to make sure the command is, in fact, requested. If so, the message is sent to the site on two modems (with different power supplies and geographically diverse communications paths) and, after sending the message, erases the tone paris from its memory. The remote site, until this time, does not know the tone pairs. When the site receives and validates the message, it sends a request for confirmation back to the central processor. When Central receives this request, it checks the switch hardware again and retrieves a fresh copy of the tone pairs from the storage processor to make sure that the site got the correct tone pairs. If all these checks pass, Central issues a go-ahead message to the site, which then (if the message is validated) actually transmits the sequence to the vehicle. During this sequence of messages, if any message fails, it is retransmitted, with a check of the switch hardware before each transmission.

Let's look at some areas that could cause an accidental trigger:

- 1. Failure of switch hardware. This would take at least six circuits failing to the "1" state, while 12 others connected to them would have to NOT fail.
- 2. Central software error. There is a lot of reliability checking, details of which are too long to repeat here; but even if there is a hole through it, the central program cannot get the tone pairs unless the switch is thrown!
- 3. Site software error. Doesn't have the tone pairs until sent by Central.
- 4. Destruct receiver failure. I didn't work with this directly (being strictly on the ground side) but everything I've seen makes them look very reliable and fail-safe.
- 5. External sabotage. A hostile agent would have to (1) steal the tone pairs, and (2) overpower our 10 kw CW transmitters which are saturating the destruct receivers with a 70 dB margin. Alternatively, if someone tried to overpower the central area, I think they would fail. Security is TIGHT around the central control area; I don't think I can go into detail without upsetting NASA and the Air Force.
- 7. Internal sabotage. One thing I did was to imagine that I was a saboteur and think of a way that I could program in a Trojan Horse to send a false command. Eventually, the system was such that I could not do it. NASA also hired an independent contractor to perform reliability analyses. NOBODY can send a command except the Range Safety Officer when he throws the switch.

The Challenger explosion was NOT caused by the Range Safety system, either intentional or accidental.

I am really sorry about the length of this message, but I wanted to get all of that in. All information contained herein is UNOFFICIAL and furnished for information purposes only. It is in no way official information from my employer (RCA), the U.S. Air Force, NASA, or any other government agency.

Due to the sensitive nature of this incident, this article is not for reproduction or retransmittal without the express permission of the author. Permission is hereby granted to Peter G. Neumann to include this material in the RISKS electronic mail digest.

> Martin J. Moore mooremj@eglin-vax.arpa

[MARTIN: MANY THANKS FOR THIS EXTRAORDINARY MESSAGE. READERS: PLEASE OBSERVE THE ABOVE CAVEAT SCRUPULOUSLY. PGNeumann]

K Re: news: Challenger lost (and note on self-destruct mechanism)

29 Jan 86 12:41:53 EST

[I presume this is from Earle S. Kyle, Jr... PGN]

Your mention of a destruct mechanism on airliners to foil hijackers raises the question of possible terrorist activity in the shuttle explosion. With the recent flap involving Libya, how certain are we that the radio code that the Air Force range safety officer uses to destruct shuttles gone astray was not compromised?

Although the slow motion video indicates some other mechanism besides on board explosives initiating the destruction of the vehicle, 1'm wondering if a high powered rifle bullet hit either the main fuel tank or one of the solid boosters shortly after launch if that could have given the same result we saw yesterday. What makes me think of that is the following: When I went to the 4th shuttle launch (STS-4), I noticed that things were quite different in the press site area (where I was) than it was for the two Apollo launches I attented (A-11, & A-17) in that same area. The difference at STS-4 was the large number of armed guards. When I asked about that, the reply was something to the effect that there had been some intelligence that someone with a high powered rifle might try to shoot at the thing during takeoff. As the shuttle flights got more routine, I'm wondering if the security at the site got a bit lax?

Does anyone know if a rifle shot on the big tank would be enough to structurally weaken it such that during that portion of the launch with maximum stress the thing might rupture?

Challenger ICING !!!

Werner Uhrig <CMP.WERNER@R20.UTEXAS.EDU> Tue 28 Jan 86 14:42:45-CST

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. Now while I have a healthy scepticism of news-coverage, and the highest respect for NASA-efforts and diligence, I still keep pondering the following news-tidbits:

- 1) ICICLES (!!!), several inches long, were shown, supposedly filmed on the launch pad or launch-vehicle this morning.
- 2) NASA sources were quoted as not being concerned very much any more when temperature rose above freezing around 10am.
- 3) NASA was quoted as having been concerned about icicles breaking off during flight and puncturing some part of the craft during launch. No mention was made of any concern either about "the extra weight" or "the effect on flight surfaces".

- 4) Some observers were commenting that the launch seemed to lift slower than usual (extra weight ??).
- 5) The explosion seemed to occur when the shuttle's 3 engines were switched to "maximum - or 104% - thrust", and on my TV, seemed to occur at the point where Challenger is connected to the external tank. Could there have been an extra stress imposed on connecting fuel-lines due to a "larger than usual differential of acceleration push excerted by the solid-fuel-rocket asembly, to which the external tank is (solidly) connected, and the shuttle vehicle, due to the additional weight of ice on the vehicles?

I assume you all are similarly puzzled about things and, maybe, made other observations that escaped me, which I, for one, would be most interested to reading

I sure hope it wasn't icing, the main killer of pilots

NO cheers today from me,)-: Werner

🗡 Big Brother, again

"Col. G. L. Sicherman" <colonel%buffalo.csnet@CSNET-RELAY.ARPA> Wed, 29 Jan 86 11:43:25 EST

I sympathize with Keith Lynch (KFL@MC.LCS.MIT.EDU)'s argument (1:40). All the same, some of his assumptions can be challenged. For example:

The character of people in government today is very
 different from 200 years ago. It is obvious that the signers
 of the constitution would have extended their protections of
 papers and places to computer files and disks, had they heard
 of such things. ... Had radio, TV, electronic funds transfer
 systems, and telephones been around in the days of Jefferson
 and Washington, I am sure that they would enjoy similar
 constitutional protection.

The structure of the U.S. government is formed for a people who get most of their information from the press. When most communication was oral, federal government was unthinkable, because nobody knew or cared about what was going on 1,000 miles away! At the same time, there was little need to "protect" expression that consisted of talking to a few friends. It was a form of communication that disappeared instantly except in the minds of one's friends; there was no enduring record to catch the eye of a jealous ruler or set before a court.

The novel idea that the government ought not to prosecute _anything_ one printed arose naturally from the nature of print consumption. Reading is something one does in _private;_ it allows one to weigh conflicting ideas without getting caught up in rhetoric. (Print has often been blamed for the decay of rhetoric!) Moreover, books as a medium have no side effects. If a book insults you, you can shut it up--something you cannot always do to a patron in a bar or on the Net.

So I agree that the founding fathers would have protected the new media, but only because they would not have understood the media's implications. Printing was always an instrument of _mass_ communication: one person talking to thousands. There's an inherent, even ridiculous imbalance in such a medium. Nevertheless, it was adopted as the basis of U.S. democracy because it was an improvement over word of mouth, and clearly "here to stay"--until something better came along.

Electronic communication is instantaneous and ephemeral. To the men of 1789, it was "obvious" that the press (and public speech) ought to be protected, and that checks and balances were needed in a representative government. To users of the Net, it is just as "obvious" that we can govern ourselves, instead of electing weirdos and crooks to "represent" us.

Col. G. L. Sicherman UU: ...{rocksvax|decvax}!sunybcs!colonel CS: colonel@buffalo-cs BI: csdsicher@sunyabva



Search RISKS using swish-e

Report problems with the web pages to the maintainer



Reliability of Shuttle SRB/MFT self-destruct mechanisms

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

Wed, 29 Jan 86 17:54:23 EST

To: mooremj@EGLIN-VAX.ARPA cc: "RISKS-LIST:"@MC.LCS.MIT.EDU, risks@SRI-CSL.ARPA

Thanks for your piece. Can you discuss at all the actual devices used on the SRBs and the External Tank to set off explosions? What ensures that they work as expected?

Reliability of Shuttle SRB/MFT self-destruct mechanisms

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

To: "lin" <lin@mit-mc> cc: <risks@sri-csl>

Unfortunately, I really can't (as opposed to "won't") amplify much on the actual destruct hardware; as I said, I worked strictly on the ground system, and I have little knowledge of explosives. My exposure to it was pretty much limited to having one of the engineers on that side show me a block diagram of the system and point out the salient characteristics...like everything else that I ever saw in this system, there were double (or more) backup paths for everything. Sorry I can't be of more help here.

The one all-pervading factor that I encountered in various mission-critical systems at Cape Canaveral is redundancy. Aside from double and triple circuitry and paths, there are two complete systems for everything; both run at all times, accepting all inputs, but only one is "on-line" with respect to outputs; if the on-line system fails (say in a power failure), the backup takes over. Or a switchover can be requested manually, or the on-line program can deliberately request a switchover if it encounters a hardware or software error.

From time to time system redundancy was tested by running a mission simulation and suddenly cutting off one power source completely. The other set of systems was fully capable of supporting the entire mission (of course, the first time we tried this -- long before the first live use of the system -we did find some problems, e.g., one system had all of its modems on the same power source. Its backup processor ran, but was deaf and dumb!) Having seen this done -- first with one power source and then the other, thus shutting down every piece of equipment at some point -- I can say that I *know* there is no single point of failure among the major system components. I would also say that unless you run such a test, you *can't* know it; you may think it, but you can't know it.

mjm

[Of course, even if you run such a test, you still may not KNOW IT... You may never know that the test was complete. PGN]

Challenger speculation

Herb Lin <<u>LIN@MC.LCS.MIT.EDU</u>> Wed, 29 Jan 86 18:18:19 EST

To: kyle.wbst@XEROX.COM cc: LIN@MC.LCS.MIT.EDU, "RISKS-LIST:"@MC.LCS.MIT.EDU, aviation@R20.UTEXAS.EDU, CMP.WERNER@R20.UTEXAS.EDU, neumann@SRI-CSL.ARPA

From: kyle.wbst at Xerox.COM

Does anyone know if a rifle shot on the big tank would be enough to structurally weaken it such that during that portion of the launch with maximum stress the thing might rupture?

It is obvious that at the time of the explosion, no rifle bullet hit it. Thus, any shot must have been fired much sooner. The rifle shot must then be timed in such a way that it is fast enough to weaken the casing, but not strong enough to penetrate it. It seems that that window is pretty small.

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.



Search RISKS using swish-e

Report problems with the web pages to the maintainer



Kisks from discussing Reliability of Shuttle Destruct System

<<u>cbosgd!akgua!whuxlm!whuxcc!crash@ucbvax.berkeley.edu</u>> Thu, 30 Jan 86 07:51:58 PST

As I read the article [by Martin Moore in <u>RISKS-1.43</u>,] 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. I had no prior knowledge of this system and now I know, generally, how it works, it's redundancy level, and it's physical location.

I am aware that much of the technical information about the shuttle is a matter of public record. I don't know what sort of information is public and what isn't. 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.

Respectfully, John Carpenter

Risks from discussing Reliability of Shuttle Destruct System

Peter G. Neumann <<u>Neumann@SRI-CSL.ARPA</u>> Thu 30 Jan 86 10:49:44-PST

To: cbosgd!akgua!whuxlm!whuxcc!crash@UCBVAX.BERKELEY.EDU cc: RISKS@SRI-CSL.ARPA

Your concern is of course very valid. The existence of such a mechanism represents a serious risk. The details of how that mechanism are thought not to be spoofable or accidentally triggered are of course the subject of an age-old controversy. On one hand, pretending that such a mechanism is safe because it is not publically known is disastrous -- especially if the mechanism is intrinsically not safe. On the other hand, publishing the details of a mechanism that is not entirely sound is also dangerous, because it may suggest the flaws to an interloper. However, unless there can be scrutiny by dedicated experts, the flaws will persist. A further comment in this chain of reasoning is that no mechanism can be guaranteed 100% sound -there are ALWAYS circumstances outside of the set of assumptions. On balance, openness appears preferable, tempered by the recognition that if the risks are otherwise too great, then what is being done should probably NOT BE DONE THAT WAY AT ALL. This is a very difficult problem, and I and many of my colleagues seem to come down fairly consistently on the side of forthright discussion rather than hiding one's head in the sand under a blanket of obliviousness. What you don't know CAN hurt you. What you do know can also. There are no easy answers. Peter

[I use "safe" and "sound" loosely to imply reliable, available, secure, nonspoofable, nontamperable, free of Trojan horses, etc.]

Possible triggering of the self-destruct mechanism

Peter G. Neumann <<u>Neumann@SRI-CSL.ARPA</u>> 30 Jan 86 09:23:53 PST (Thu)

Much to my surprise -- since it did not seem too likely -- I heard of a report on the radio last night by a physicist (and head of a company that does something with solid-fuel rockets) who speculated that the explosion in the solid-fuel rocket booster set off the self-destruct mechanism, resulting in the destruction of the orbiter. He suggested that it could not have been a hydrogen leak because hydrogen burns clear and the Shuttle explosion had an obvious orange glow.

Main The Challenger [non]accident

Jeff Siegal <<u>JBS%DEEP-THOUGHT@mit-eddie.MIT.EDU</u>> Thu 30 Jan 86 20:22:37-EST

To: RISKS%SRI-CSL@EDDIE.MIT.EDU Cc: LIN@MC.LCS.MIT.EDU

From: Herb Lin at MC.LCS.MIT.EDU

It is obvious that at the time of the explosion, no rifle bullet hit it. Thus, any shot must have been fired much sooner. The rifle shot must then be timed in such a way that it is fast enough to weaken the casing, but not strong enough to penetrate it. It seems that that window is pretty small.

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.

I have, in general, been concerned about the fact that, except for a single question asked by one reporter at the first news conference, there has been no public mention of the possiblity of terrorism.

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 haven't noticed any great measure of security (except DoD flights), but perhaps this has been the result a NASA P.R. effort make the Space program appear as "open" as possible.

Jeff Siegal

Shuttle Explosion -- Plutonium on Galileo

<<u>LShilkoff.ES@Xerox.COM</u>> Thu, 30 Jan 86 17:05 PST

To: "risks" <risks@sri-csl.ARPA>

I understand the Galileo probe which was planned to be on a shuttle flight this summer is powered by plutonium. Had Galileo been on this flight, it seems to me a whole bunch of plutonium particles would have been raining along the coast of Florida.

Any comments?

Larry

Reliability in redundant systems

Brad Davis <<u>b-davis@utah-cs.ARPA</u> > Thu, 30 Jan 86 09:08:52 MST

Martin Moore's report on the self destruct devices was very informative. 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.

Brad Davis



Search RISKS using swish-e

Report problems with the web pages to the maintainer