Search RISKS using swish-e

THE RISKS DIGEST

Forum on Risks to the Public in Computers and Related Systems

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

Index to Volume 5

Thursday, 31 December 1987

Forum on Risks to the Public in Computers and Related Systems

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

THE RISKS DIGEST

Forum On Risks To The Public In Computers And Related Systems

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

Search RISKS using swish-e

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

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

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

Feeds

RSS 1.0 (full text)

RSS 2.0 (full text)

ATOM (full text)

RDF feed

WAP (latest issue)

Simplified (latest issue)

Smartphone (latest issue)
Under Development!!

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

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

Selectors for locating a particular issue from a volume

Volume number: Volume Issue Number: Issue

Get Specific Issue

Volume Index

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

Index to the RISKS Digest

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

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

Search RISKS using swish-e

THE RISKS DIGEST

Forum on Risks to the Public in Computers and Related Systems

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

Volume 5: Issue 1

Forum on Risks to the Public in Computers and Related Systems

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

This issue does not exist.

Search RISKS using swish-e

Report problems with the web pages to the maintainer

Search RISKS using swish-e

THE RISKS DIGEST

Forum on Risks to the Public in Computers and Related Systems

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

Volume 5: Issue 1

Forum on Risks to the Public in Computers and Related Systems

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

This issue does not exist.

Search RISKS using swish-e

Report problems with the web pages to the maintainer

Search RISKS using swish-e

THE RISKS DIGEST

Forum on Risks to the Public in Computers and Related Systems

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

Volume 5: Issue 2

Friday, 12 June 1987

Contents

Three gremlins on the loose: nukes, sharks, enlightened rockets

Dave Platt <dplatt@teknowledge-vaxc.ARPA>
Thu, 11 Jun 87 08:08:13 pdt

[Whereas the following three incidents are not directly computer related, they are clearly RISKS related, providing further examples of the unexpected technical failures. On examining my list of collected cases, I am astounded to discover how many of the cases were due to causes that (a) had never occurred before and (b) no one had even anticipated might occur. PGN]

This morning's San Jose Mercury News contains three interesting articles, almost one-after-another. Their headlines, and a summary of their contents:

* "Official says many U.S. atom bombs are faulty"

More than one of every three nuclear weapons in the U.S. arsenal doesn't work properly, [Sylvester Foley, asst. sec. of energy for defense programs] said yesterday [during a breakfast meeting with reporters].

"Hypothetically, it could be catastrophic if you ever wanted to use it and you pushed the button and nothing happened", said Foley.

{ no comment... dcp }

* "Jaws V: Sharks make light lunch of trans-Atlantic fiber-optic cables"

Sharks seem to have taken a fancy for the new 1"-thick underwater cables being strung across the Atlantic; they've bitten through the cable at least four times (cost-to-repair $250,000 per bite). Similar bitings have been reported in the Pacific. Older-style copper-wire cables apparently weren't attractive to sharks, and weren't bitten.

[The NYTimes article suggests that the sharks seem to be attracted to the low electrical currents in the copper wires providing power for the fiberoptic repeaters. The new cables are still shielded, but much thinner than previously. PGN]

* "Lightning hits NASA launch pad inadvertently setting off 3 rockets"

A lightning strike on a pad at NASA's launch facility at Wallops Island, VA. ignited three small rockets and sent two of them hurtling along their planned trajectories; they were more than two miles out before the NASA officials could prepare to track them. The third rocket wasn't in firing position, and splashed down in the ocean 300 feet from the pad. It appears that a lightning bolt may have induced a current pulse in the firing leads, triggering the igniters.

One of the rockets was scheduled to have been launched shortly thereafter to study night-time thunderstorms and their effect on the atmosphere.

[The weather-satellite ground station was also affected, despite surge suppressors and grounding wires that were supposed to protect it. Weather data from GOES-West could not be received for 9 hours, and GOES-East was blacked out for 5.5 hours. NYTimes, same day. PGN]

Yet another air-traffic-controller foul-up

Roy Smith <cmcl2!phri!roy@seismo.CSS.GOV>
9 Jun 87 20:24:16 GMT

From the NY Times, June 9, 1987, page A22: "Coding Error at O'Hare Brings Two Jets Much Too Close Together". Comments/elipsis in [brackets] are my summations or deletions from the original.

"Two American Airlines jets were guided past each other at a fraction of the minimum legal distance of separation between them because of an error by an air traffic assistant, the National Transportation Safety Board said yesterday. [This happened late last month.]

"But Mr. Engen [chief of the F.A.A.] said he did not believe that

the incident justified any permanent reduction of, or special restraints on, Chicago area traffic. He said the F.A.A. had determined that existing procedures, "when properly applied, do maintain a safe level of operation in the Chicago area." [...]

"According to officials of the safety board and the F.A.A., here is what happened:

"An air traffic assistant in the tower at Chicago's O'Hare Internation Airport assigned the wrong code to the crew of a United Airlines plane that was about to take off. The code was the one for an American Airlines plane that took off three minutes later.

"Result: Confusion

"The result was that the full-fledged controller whose job it was to radio subsequent air traffic instructions to the two planes saw the United plane on his radar scope with the American plane's identification, altitude and other data. The computer feeding this data to the radar scope rejected duplicate data for the American plane, rightly concluding that two planes could not have the same code. The American plan showed up only as a bright radar blip, without any identification alongside.

"Now, the controller wanted the United plane, with the American plane's data next to it, to climb to a new altitude. When he radioed instructions to "American 637" to climb, the United crew ignored them, and the instruction were carried out by the real American 637. [This caused American 637 to pass another American plane at 1/4 mile horizonal and 500 feet vertical separation -- the rules call for 3 miles and 1000 feet.]

"[The quick fix is to add more supervisory staff to the O'Hare tower.]

The biggest question in my mind is why does the system just drop one plane if it sees two with the same id? Shouldn't bells ring and lights flash when an obvious operator-error situation like this pops up? Also, why isn't the plane id part of the info sent by the on-board transponder? Aren't these id's simply the flight numbers assigned by the airlines? Why should it require any manual intervention to assign an id to a blip?

Roy Smith, {allegra,cmcl2,philabs}!phri!roy
System Administrator, Public Health Research Institute
455 First Avenue, New York, NY 10016

National Crime Information Center access

Peter G. Neumann <Neumann@CSL.SRI.COM>
Fri 12 Jun 87 07:27:29-PDT

Also in the NYTimes on the same day as the bombs, the sharks, and the enlightning rockets was a front-page item on a proposed expansion of the

NCIC database that would permit Federal, state, and local law-enforcement agencies to exchange information on people who are suspected of a crime but have not been charged. A government advisory panel also recommended that the NCIC should have access to other databases such as those of the Securities and Exchange Commission, the Internal Revenue Service, the Immigration and Naturalization Service, Social Security, and State Department passport office. Attempts to legislate controls were also noted in the Times article, although concerns for protection of privacy seemed not to be commensurate with inadequacies in the technology and practice of protecting systems and networks from internal and external misuse. PGN

Yes, Virginia, There Are Software Problems

Nick Condyles <condyles@talos.UUCP>
8 Jun 87 20:46:10 GMT

The following appeared in the Richmond Times-Dispatch June 8, 1987 Section B page 1. The article pertains to the state of Virginia's attempt to automate distribution of child support payments.

STATE PAYMENTS FOR SOFTWARE SYSTEM HALTED

State officials have halted payments on a problem-plagued computer software system used in distributing child support checks and say the manufacturer will get no more money until the system works.

The state secretary of human resources, Eva S. Teig, said Saturday that the state has paid Unisys Inc. only $75,000 of the $395,000 total "because we are not satisfied with the product. Until we are satisfied, we will not continue payments on the program."

Ms. Teig's announcement came as she prepared to submit a confidential report on the child-support automation problems to Gov. Gerald L. Baliles. The report "is a look at what has happened and a recommendation on where I think we should be going," she said.

The software system has been blamed for massive snarls in the distribution of child support checks.

If state officials are unable to work out the problems, Ms. Teig said, "we'll look at other alternatives. We're committed to making it work."

Del. Howard E. Copeland, D-Norfolk, last month asked Attorney General Mary Sue Terry to investigate the state Department of Social Services' purchase of the software and determine whether it has been acquired through legal procedures.

Bert Rohrer, a spokesman for the attorney general, refused to comment on whether an inquiry is being conducted.

The purchase of the software was part of the department's attempt to

take over collection of child support payments, a job that had been done by the courts. The centralization brought widespread complaints about lost checks, delayed payments and improper seizure of tax refunds.

Social Services Commissioner William L. Lukhard approved the purchase of the software system from Unisys, formerly Sperry Corp., in May 1985. Critics say the software never worked properly, causing further delays in the already slow distribution of checks.

A federal audit last month said operating the new computer system would cost Virginia up to $7 million per year, more than three times the amount originally anticipated.

Representatives of Unisys and state computer experts are analyzing the system to determine if it can be corrected and "some progress has been made," Ms. Teig said.

The state is prepared to take further action if the software cannot be salvaged, Ms. Teig said. She would not elaborate.

Several state legislators have suggested that Lukhard be replaced as social services commissioner.

"As I've said before, I think the best thing for the whole department is someone who would come in with a new broom and sweep clean," said Del. Frank D. Hargrove, R-Hanover. "The buck stops at the boss's desk."

Others defended the agency chief. "I would be disappointed and upset if he was driven out of office," said Sen. Joseph V. Gartlan Jr., D-Fairfax. "I regard him as one of the best administrators in state government."

Nick Condyles

Tue <Date: 09 Jun 87 13:58:02 PDT>
Tue, 9 Jun 87 17:42:20 PDT

Regarding your Contributions from the Editor in SEN on Heisenbugs (RISKS and SEN v12, n 2, Apr. 1987):

I felt I should bring to your attention the major problems in the area of concurrent or parallel computing. I am concerned because too many people are using the buzzword of "parallel computing" without fully understanding the consequences (not just in the supercomputing disciplines).

Many people are making vast assumptions on the synchrony and determinism of such systems and on the ability of new compilers to utilize vector and parallel processing. I wish to point this problem out because as parallel architectures move into the work space, these problems will increase and they are moving into areas such as SDI which have serious consequences.

One sub-problem I have noticed in debugging parallel codes is that many of the existing software engineering tools and methodologies are very sequentially oriented. I have noted sequential version numbering of certain file systems (manufacturers will not be mentioned) are great hinderances in working in highly parallel environments.

The problem of Heisenbugs is not entirely new in this realm, and I would like to point out significant technical report released some time ago on the problem:

%A Dale H. Grit
%A James R. McGraw
%T Programming Divide and Conquer on a Multiprocessor
%R UCRL-88710
%I Lawrence Livermore National Laboratory
%C Livermore, CA
%D May 1983
%X Test programming the Denelcor HEP using HEP asynchronous FORTRAN. Has interesting insights to MIMD programming of the future.

This paper does have other antecedents (such as the Computing Surveys article by Anita Jones on multiprocessor experiences [1980]), but the above paper points out an attempt at debugging a program which completely interfered with (improved) the functioning of a buggy program. Languages like Ada(tm) cannot be expected to completely solve these problems, nor can their support environments, since these problems are still in the realm of open research issues.

Heisenbugs won't be restricted to parallel programs. Non-deterministic, self-modifying artificial intelligence programs also have the potential have showing these behaviors.

--eugene miya
NASA Ames Research Center
eugene@ames-aurora.ARPA
"You trust the `reply' command with all those different mailers out there?"
{hplabs,hao,ihnp4,decwrl,allegra,tektronix,menlo70}!ames!aurora!eugene

Additionally, I add the file I have on the risks of supercomputers:

Perspective:
Supercomputer is just a marketing term -- Enrico Clementi (IBM)

Definition:
A supercomputer is typically defined as the fast computer at a given point in time.
Another definition is any computer which turns a CPU-bound problem into an I/O-bound problem. {Ken Batcher}

Risks of supercomputing

1) User bites off more computation than can chew: 27 hours weather for 24 hour forecast. Supercomputers and parallel processors are O(n)

solutions for O(n^3) problems in some cases. Danger of the space filled by the computation (take the space or what ever). It is also known, now, that the NWS can be liable for weather forecasts.

2) Lack of software and the fact it is state of the art hardware (tends to be not as well shaken out) not necessary fault-tolerant (PEPE [a BMD computer] might have been an exception). The typical supercomputer application tends to be behind the software engineering art.

3) A perceptual power trip problem: most powerful thing we have can handle ANYTHING. Stop thinking and do more computing.

4) Normal risks inherent in all computer analysis and simulation: bad data, incorrect models, only faster, and in some cases harder to detect errors.

5) Many of the newest designs are using radically different architectures: hypercubes, ensembles like the Connection machine, shared memory systems, hardware semiphores like the HEP, data flow machines, ELI (or VLIW) machines, vector processors and so forth. Programming applications for these machines has been described as programming in 1946. A comment ascribed to Steve Squires of DARPA attributed that perhaps only 20% of programmers out there could make the transition to working on these new machines. It's not just loop or recursion problems, consider staravation and deadlock in applications programs. People waiting for smart compilers better not hold their breath. You should remain skeptical of any claim of sophistication (i.e., drop your dusty deck in this machine).

A problem I have: tools designed for sequential programming environments are difficult to use in parallel environments. The VMS/RSX version numbering system is a real pain because it has a serial numbering. This is a bottleneck for some of my programs.

Lastly:
n) The physical embodiment problem (Ken Thompson): harm by dropping out of a plane. (A mention of this problems with the Belle chess machine: a specialied architecture, but not a super).

Search RISKS using swish-e

THE RISKS DIGEST

Forum on Risks to the Public in Computers and Related Systems

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

Volume 5: Issue 3

Thursday, 18 June 1987

Contents

Australian ATM troubles...

David Purdue <munnari!csadfa.oz!davidp@seismo.CSS.GOV>
Tue, 16 Jun 87 16:53:04 est

First some background: The Westpac Bank installed a new software system for its ATM's which did not do proper checking. Thus it allowed people to withdraw more than the daily maximum allowed ($200). It even allowed the withdrawl of more than was held in the account. The ATM's were supposed to allow customers of the Commonwealth Bank to access their accounts, but this access was denied by the new software.

From "The Canberra Times", Tuesday, June 16, 1987.

BANK LOSES HEAVILY IN AUTO-TELLER 'HICCUP'

Westpac's troubles began on Saturday, May 30, when programmers installed the IMS version 2.2 of IBM's software. The following Thursday, after a week long crisis, Westpac decided to close all its automatic tellers throughout Australia, suspecting widespread fraud. Because of the costs of recovering debts, Mr Paget said the bank would probably not take legal action to get its money back from people who were unable to repay it.

The Federal Treasury ordered an immediate inquiry on the situation as it developed. "We were concerned for the cardholder where there was a technical malfunction and the cardholder lost money," a Treasury official said. However he warned that the Treasury might get involved again if legitimate customers had rights abused during that period.

It seems the "hiccup" was more extensive than first reported. "Computing Australia" was told by Mr John Kosh, assistant manager of electronic banking for the Commonwealth Bank, that the Westpac system was malfuctioning for the whole of the week before Westpac closed the machines.

Because of this, he said, Commonwealth cardholders had been unable to use Westpac automatic tellers. At first, the Commonwealth believed it to be a communications problem. "We didn't know what was happening," he said.

The SWIFT network for the international transfer of funds was also hit, with Westpac unable to send funds overseas while the host computer was down. Mr Paget said this caused "some inconvenience" to corporate customers.

Westpac has blamed insufficient software testing for the disaster and maintains it will reinstall the offending software later. Mr Paget admitted that "somehow or other the testing didn't cover the problem".

"The new software is back with the technicians: we're saying we don't like what happened, and we don't want this to happen again," he said. "There's no doubt it will go back in at some stage, but they've got to find out why it didn't work and try to work out how to fix it. From where I sit, we'll be looking at test upon test upon test."

He said Westpac would not seek compensation from IBM. "When you are in a long term relationship with a supplier, this is going to happen," Mr Paget said. "Our people were involved with the software all the way along. We have to be big boys and live with it."

DavidP

Mr. David Purdue Phone ISD: +61 62 68 8165
Dept. Computer Science Telex: ADFADM AA62030
University College ACSNET/CSNET: davidp@csadfa.oz
Aust. Defence Force Academy UUCP: ...!seismo!munnari!csadfa.oz!davidp
Canberra. ACT. 2600. ARPA: davidp%csadfa.oz@SEISMO.CSS.GOV
AUSTRALIA JANET: davidp@oz.csadfa

Australian ATMs... [Another version!]

Dave Horsfall <munnari!astra.necisa.oz!dave@seismo.CSS.GOV>
11 Jun 87 09:29:38 +1000 (Thu)

Although stories about bank ATM's swallowing customer's money are common enough, you don't see too many stories about the opposite situation happening. Here is a story from the "Sydney Morning Herald" (Sydney, Australia) dated Friday 5th June:

> The day Westpac's computer gave away money
>
> Westpac Banking Corporation is believed to have lost millions of dollars in international transactions, and will be forced to recover an undisclosed amount from customers who withdrew unauthorised cash from automatic teller machines, following a serious fault in the bank's computer system.
>
> A major failure in a new software system introduced last weekend forced the closure of all the bank's 650 automatic teller machines (ATMs) across Australia yesterday. The fault also affected other ATMs with which the Westpac computer is linked.
>
> After the fault developed earlier in the week, customers suddenly found themselves able to make multiple withdrawals of amounts beyond the usual daily limit of $200, even if the account held no money. They were also able to withdraw from cheque accounts they did not have.

The article went on to describe how "normally impoverished inner-city types (were) suddenly treating themselves to cocktails in expensive restaurants and buying new clothes at the QVB (a trendy boutique)", and that the SWIFT system (Society of Worldwide International Financial Transactions) was inaccessible. However, the bank denies losing millions of dollars this way.

Apparently, parts of the new software could not cope with carrying three or four times the number of transactions they had been tested for, and the ATMs were forced to work in isolation, unable to communicate with the host processor. This raises a few important points:

1) Why was the real-life situation so much worse than what had been expected? Don't banks test software until it fails?

2) Why were the ATMs permitted to work on their own, happily dispensing cash from empty accounts?

And more importantly ...

3) Assuming these ATMs have an internal audit trail, how much reliance can be place on them, in order to recover the money from customers who (knowingly) defrauded them? I can see the court case now:

"But, m'lud, Westpac has ALREADY ADMITTED that its software was at fault. How can we trust these little bits of paper inside their machine, claiming that my client had defrauded them?"

ATMs *DO* have an internal audit trail, don't they?

Dave Horsfall (VK2KFU) TEL: +61 2 438-3544 FAX: +61 2 439-7036
NEC Information Systems Aust. ACS: dave@astra.necisa.oz (also CSNET)
3rd Floor, 99 Nicholson St ARPA: dave%astra.necisa.oz@seismo.css.gov
St. Leonards NSW 2064 UUCP: {enea,hplabs,mcvax,prlb2,seismo,ukc}!\
AUSTRALIA munnari!astra.necisa.oz!dave

Australian ATMs...

John Colville <munnari!nswitgould.oz!colville@seismo.CSS.GOV>
Fri, 12 Jun 87 09:17:42 EST

[...] Since then they have been running large ads in the newspapers with a funny drawing of an ATM with 'HIC' coming from its dispenser slot.

Westpac tried the new version of IMS2 against their test data transactions but not against a load approximating anything like the actual loads. (One of my students, who works with another of the Big Four banks, says that his bank always tests against live load levels before they bring in changes: perhaps reasonable validation does take place sometimes)

John Colville, N.S.W. Institute of Technology, colville@nswitgould.oz.AUS

Not paying by Access can ruin your credit limit!

Mike Bell <mcvax!camcon!mb@seismo.CSS.GOV>
12 Jun 87 09:24:03 GMT

The UK Consumers' Association magazine Which? has the following cautionary tale about use of credit cards [precis].

"Sally Allen booked into a hotel near Paris for the night. As well as taking her passport overnight, the hotel asked for her Access card. They took an imprint on a payment voucher, even though she had no intention of paying by Access, explaining that it was a safeguard against non-payment of her bill."

"When she returned home and tried to use her Access card she was refused credit, even though she had next to nothing charged on her card. She

contacted Access and demanded an explanation. Apparently the hotel in France had *reserved credit* on her account for the cost of her stay, and been given an authorisation number from the Access computer in the UK. The amount reserved had been deducted from her credit limit. The only way her credit could be restored was for the hotel to contact them, and to cancel the transaction. She wrote to the hotel immediately, but it took six weeks for the credit to be restored."

Which? reports that Access and Visa both think the hotel was operating outside the agreed conditions of use, but that because they have no direct contract with the French hotel, all they can do is lobby their respective international organisations (Mastercard and Visa International) for a ban.

Anybody else come across this problem of uncancelled "transactions"?

It seems very wrong that someone can screw up your credit without you ever signing or agreeing anything, and that the matter can't be put right because of the national boundaries involved.

Mike Bell --Email: mb%camcon.co.uk Phone: +44 223 358855
UUCP: ...seismo!mcvax!ukc!camcon!mb
Organization: Cambridge Consultants Ltd., Cambridge, UK

Ex-Directory [Arrested by unwristed phone mumbers!]

Brian Randell <brian%kelpie.newcastle.ac.uk@Cs.Ucl.AC.UK>
Wed, 17 Jun 87 10:41:34 bst

I've been told that seven terrorists (belonging to Action Directe?) were recently caught in France after the police took possession of an electronic wrist-watch/calculator in which one of the terrorists had stored a set of telephone numbers. Can anybody confirm this, and provide details? I don't recall discussion in RISKS of any such incident, and its a nice Gallic equivalent to the Irangate archived messages incident, if it's true.

Brian Randell - Computing Laboratory, University of Newcastle upon Tyne

ARPA : brian%cheviot.newcastle.ac.uk@cs.ucl.ac.uk
UUCP : <UK>!ukc!cheviot!brian
JANET : brian@uk.ac.newcastle.cheviot

Risks of Computerized Airport Gate Signs

<Chuck.Weinstock@sei.cmu.edu>
18 Jun 1987 11:12-EDT

Last night I had the pleasure(?) of trying out United Air Lines new O'Hare terminal. The terminal is extremely modern, complete with computerized departure signs for each gate (in a red color that can't be read when the sun backlights it!) In the closet behind each gate check-in counter there is an IBM PC (I think) with a menu driven

program used to set the information on the departure sign.
Unfortunately, any gate computer can control any gate sign, and the
result is that a simple operator error can cause lots of trouble.
In particular, last night, while I watched, the Pittsburgh flight
indicated behind the counter turned magically into one for Columbus.

I should also point out that the low tech solution of a sign board to
be slipped into a slot took only about 30 seconds per flight
changeover. I watched the attendent take almost 5 minutes to
changeover under the new and improved high-tech solution. (To be fair,
the terminal has only been operating since Monday.)

Aside: if you are unfortunate enough to have to connect from United
gates E-F to United gates B, plan on missing your flight unless you've
added an extra 15-20 minutes for the hike. The terminal won't be fully
operational until 1989, though much UAL operations will switch there in
August of this year.

DMV Computer Changes Names

"IMS/John Mulhollen" <johnm@afsc-bmo.arpa>
11-JUN-1987 16:33 PDT

Article in 11 June 1987 Los Angeles Times:

> "N.J. Computer Gives Drivers the Business
>
> "Trenton, N.J. - Hundreds of drivers who notified Department of Motor
> Vehicles last month of new addresses found that a computer had changed
> their names -- to Watkins Leasing Co.
>
> "The computer error has been corrected and new address labels are being
> sent this week to all of the drivers affected, a department spokesman said.
>
> "Watkins Leasing Co. is a truck dealership and leasing concern with
> offices in Chester, PA and Wilmington and Harrington, Del."

Interesting. Why Watkins Leasing Co since apparently Watkins isn't even
located in New Jersey??? JohnM

UHB demonstrator flight aborted by software error

<Peter G. Neumann <Neumann@csl.sri.com> [from Kenneth R. Jongsma]>
Thu 18 Jun 87 21:12:52-PDT

On 18 May 87 a demonstrator flight of the McDonnell Douglas UHB twin-jet
(with one GE prototype unducted fan engine) was cut short when a cockpit
light indicated a potential problem with the UDF engine. The warning was
triggered by a pressure sensor when the aircraft climbed above 12,000 feet.
Subsequent testing showed there was a software error in the annunciation logic.

[Source: Aviation Week & Space Technology, 1 June 87, courtesy of Kenneth R. Jongsma]

Yet another air-traffic-controller foul-up (revisited)

Joe Morris (jcmorris@mitre.arpa) <jcmorris@mitre.arpa>
Mon, 15 Jun 87 11:33:42 EDT

A short tutorial on aircraft transponders...

In RISKS 5:2 Roy Smith asks:

<> ...why isn't the plane part of the info sent by the on-board transponder?
<> Aren't these id's simply the flight numbers assigned by the airlines? Why
<> should it require any manual intervention to assign an id to a blip?

The transponder presently in use by all aircraft in the US has been around for many years. It has the ability to:

- Receive an unaddressed query pulse from a ground radar site and respond with a pulse of its own.

- Include with its response the transponder code set by the pilot. (This is the code which was incorrectly assigned at O'Hare.) The code is a 4-digit octal number, and has no relationship to the aircraft registration number or the (airline-assigned) flight number.

- Report if a special button (marked IDENTIFICATION) has been pressed within the past few seconds. This can be used by a controller to positively identify an aircraft, since its receipt causes the radar display to change the shape of the blip which represents the return.

- Report the pressure altitude of the aircraft, referenced to a barometer setting of 29.92" Hg. This ability is not required in low-altitude flights and is an extra-cost feature.

Work is being completed by the FAA on a replacement for the present transponder design. The new transponders (called "Mode S") will include a permanently-assigned identification, unique to the aircraft, which will be transmitted along with the other data when the transponder decodes a query. Until the Mode S gear comes into use, however, we are still limited to a transponder code address space of 4096 discrete codes to identify an aircraft.

The effective address space is smaller, since several blocks of 100(8) are reserved for special purpose. Code 1200 is the general VFR (visual, not under radar control) code; 75xx, 76xx, and 77xx are emergency codes, and so forth.

A feature of most radar display systems is the ability to use the transponder codes to DE-select a return so that a controller's display does not show the transponder data for aircraft not under his/her jurisdiction. Such aircraft might be separated horizontally (in another controller's sector) or vertically

(as in an overflight above an airport). In places like Southern California, this can be used to suppress the clutter caused by VFR (code 1200) aircraft which would otherwise obscure the returns of controlled aircraft. It has been reported (and denied) that the controller involved in the Cerritos crash had suppressed the VFR returns such as that of the intruding Piper.

Yes, it would be nice if the system could set off alarms when the data became ambiguous. But at what point should it delay the alarm against the possibility of a transient failure (e.g., the second aircraft might have been changing the code setting and been on AA637's code just as the radar beam swept past)? A real problem in aviation system engineering is the incredible number of alarms which some pilots consider to be a safety risk in themselves since they can go off in combinations which distract the aircrew.

There's an O*L*D joke about the pilot who was hauled up before a board after landing his airplane with the landing gear still up. His defence was that the gear-up warning horn was so loud that he was distracted from performing the "gear down and locked" item in his pre-landing checklist.

Joe Morris (jcmorris@mitre.arpa)

Aircraft Transponders and Errors in Setting Codes [Some duplication]

Paul A. Suhler <suhler@im4u.utexas.edu>
Fri, 12 Jun 87 16:07:31 cdt

Before takeoff on an IFR (instrument flight rules) flight, an aircraft's pilot is given a "squawk", a four octal digit code to enter into his transponder. This is also entered into the ATC system's computer so the code returned by the transponder when interrogated by radar is automatically translated into the airline and flight number displayed on the controller's radar scope.

As there are 4096 possible codes and probably lots more aircraft flying IFR than that, pilots sometimes have to change squawks in mid-flight when going from one region to another. And, as airlines have duplicate flight numbers that range from one to four decimal digits, they can't use those for their squawks. [...]

VFR aircraft receiving terminal radar service also use this facility, although they are only using it at the beginning and end of the flight. Also, codes 75XX are reserved for hijacked aircraft, 76XX for those with communication failures, and 77XX for those declaring emergencies, so that the total number of squawks available is actually less than 4096.

Paul Suhler suhler@im4u.UTEXAS.EDU 512-474-9517/471-3903
Organization: Univ of Texas Elec & Comp Engr Dept

On the bright side, at least my computer still works...

Jon Jacky <jon@june.cs.washington.edu>
Wed, 17 Jun 87 20:36:02 PDT

I got an ad from Raytheon today for a Mil-Spec version of the VAX (built under license from DEC). It is described as an "extreme performance machine which survives tactical levels of nuclear weapons effects (NWE)."

On a related note, the June 15, 1987 issue of the trade paper ELECTRONIC ENGINEERING TIMES has an article called "Reveille for Military ASICs" (by Terry Costlow, pps. 1 and 16). It notes "Radiation hardening has been viewed largely as an aerospace application, but it is now being included in smaller weapons that are being produced in higher volumes than one-of-a-kind spacecraft. 'We're seeing more nuclear weapons being designed for tactical battlefield conditions. In the past, rad-hard was just used in weapons like intercontinental missiles. We feel this may be a nice emerging niche', says (semiconductor vendor) NCR's (director of marketing Patrick) Riley."

Jonathan Jacky

Human Factors and Risks

"Lindsay F. Marshall" <lindsay%kelpie.newcastle.ac.uk@Cs.Ucl.AC.UK>
Mon, 15 Jun 87 9:49:41 BST

Nothing to do with computers, but a very important point for system designers. I was reading a book the other day in which the author mentions the pang of fear that struck him on a plane one day, when he noticed that the screws holding the ashtray to the seat did not match. He instantly thought "Is this how they fix the engines too??".

Moral: Attention to the cosmetic details can play a great part in re-assuring users (no matter how falsely!).

Lindsay F. Marshall, Computing Lab., U of Newcastle upon Tyne, Tyne & Wear, UK
JANET: lindsay@uk.ac.newcastle.cheviot ARPA: lindsay%cheviot.newcastle@ucl-cs
PHONE: +44-91-2329233 UUCP: <UK>!ukc!cheviot!lindsay

Re: Risks of so-called ``computer addiction''

John Mackin <munnari!basser.cs.su.oz!john@seismo.CSS.GOV>
16 Jun 87 18:09:47 GMT

I'm surprised that no one has mentioned the book ``Computer Power and Human Reason'', by Joseph Weizenbaum. Weizenbaum calls the phenomenon ``compulsive programming'', and devotes quite a large part of the book to discussion of it.

John Mackin, Basser Dept of Computer Science, Univ.of Sydney, Sydney, Australia

---

Directions and Implications of Advanced Computing

Douglas Schuler <douglas@BOEING.COM>
Thu, 18 Jun 87 13:12:36 pdt

DIRECTIONS AND IMPLICATIONS OF ADVANCED COMPUTING
A One Day Symposium - July 12, 1987
University of Washington, Seattle, Washington

PROGRAM

On-Site Registration (8:00 - 9:00)

PLENARY SESSION (9:00 - 10:30)
Robert Kahn and Terry Winograd with Gary Chapman

The featured speakers will discuss the role of funding on computer science research. How and why are projects selected for funding? What are the roles of the Department of Defense, civilian agencies and private sources? Does it matter where research money comes from?

Robert Kahn is the founder of the non-profit Corporation for National Research Initiatives, in Washington, D.C. Until 1985, Kahn was director of the Information Processing Techniques Office at the Defense Advanced Research Projects Agency (DARPA).

Terry Winograd is an associate professor of computer science at Stanford University. He is author of "Understanding Natural Language", "Language as a Cognitive Process" and (with Fernando Flores) "Understanding Computers and Cognition". Winograd is the national president of Computer Professionals for Social Responsibility (CPSR).

The discussion will be moderated by Gary Chapman, Executive Director of CPSR. He is co-editor of the book, "Computers in Battle" to be published this fall. Chapman is a former member U.S. Special Forces.

PARALLEL SESSIONS

FUNDING (11:00 - 12:00)
David Bushnell - The Promise and Reality of ARPANET: A Brief History
Joel Yudken and Barbara Simons - Project on Funding in Computer Science:
A Preliminary Report

AI PROSPECTS I (11:00 - 12:00)
Juergen Koenemann Artificial Intelligence and the Future of Work
Reinhard Keil-Slawik An Ecological Approach to Responsible
Systems Development

MILITARY/RELIABILITY (1:30 - 3:00)
Richard Hamlet - Testing for Trustworthiness
David Bella - Fault-tolerant Ballistic Missile Defense
Erik Nilsson - The Costs of Computing Star Wars

EXPERT SYSTEMS (1:30 - 3:00)
Matthew Lewis and Seth Chaikin - Will There Be Teachers in the Classroom

of the Future?
Rolf Engelbrecht - Expert Systems in Medicine - A Technology Assessment
Carole Hafner and Donald Berman - The Potential of AI to Help Solve the
Crisis in Our Legal System

RESEARCH PRIORITIES (3:30 - 4:30)
Douglas Schuler - A Civilian Computing Initiative: Three Modest Proposals
Jack Beusmans and Karen Wieckert - Artificial Intelligence and the Military

AI PROSPECTS II (3:30 - 4:30)
Susan Landau - The Responsible Use of 'Expert' Systems
K. Eric Drexler - Technologies of Danger and Wisdom

VIDEO
Daressa Computers in Context
CPSR Reliability and Risk
videotape on DBNET (a computer mail network for the deaf-blind)

REGISTRATION FEES: Regular $50, CPSR Member $30, Student/Low Income $20
Proceedings only (cannot attend symposium) $15 Proceedings will be
distributed to symposium registrants on day of symposium. Lunch is included.

DIAC '87, CPSR/Seattle, P.O. Box 85481, Seattle, WA 98105
Sponsored by Computer Professionals for Social Responsibility

---

Software Risk Management

<wallace@ICST-SE>
Thu, 18 Jun 87 08:38:21 edt

The National Security Industrial Association (NSIA), in cooperation with the National Aeronautics and SpaceAdministration (NASA), DOD, the National Bureau of Standards(NBS), the Library of Congress, Society for Software Quality, the Aerospace Industries Association of America (AIA), the G-34 Computer Resources Committee of the Electronic Industries Association (EIA), and the American Society for Quality Control, is sponsoring the Fall Joint National Conference on Software Risk Management. The conference will be held September 30 - October 2,1987 in Los Angeles at the Los Angeles Airport Hilton Towers, on Century Boulevard.

Dr. Barry Boehm of TRW will be the keynote speaker of the conference beginning at 1:30 PM on Wednesday, September 30. The conference features key government officials and world renowned speakers from academe, consortia and industry.

For information on the conference program and registration, contact Jerry Smith at QSOFT, Suite 206, 2755 Hartland Road, Falls Church, VA 22046, (703) 560-4440 or Jerry Raveling, UNISYS, Sperry Park, St. Paul, MN 55164-0525, (612) 681-6800

Report problems with the web pages to the maintainer

Search RISKS using swish-e

THE RISKS DIGEST

Forum on Risks to the Public in Computers and Related Systems

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

Volume 5: Issue 4

Wednesday, 24 June 1987

Contents

Immoderation and Nonmoderation

Peter G. Neumann <Neumann@csl.sri.com>
Tue 23 Jun 87 16:53:12-PDT

A few of you have received a UUCP message through "cbosgd" that intended to demonstrate that systems are not really very secure and that it is easy to bypass moderation on supposedly moderated news groups. (The message in question was written as a response to someone who thought that this might be difficult!) The existence of that message should not surprise any readers of RISKS, who by now have no trouble grasping the fact that there is no such thing as complete security. However, the message was sent not through RISKS@CSL but through one of our innumerable redistribution points (and thus was received by only a very small fraction of all RISKS readers). The possibility of doing that should not be a surprise, particularly in that most local redistribution centers have been explicitly set up to be automatic forwarders rather than requiring manual intervention.

A long time ago Dave Parnas objected to having his position papers on Star Wars serialized in Soft-Eng@MIT-XX and circulated via netmail, partly because there are no guarantees that the received message was actually authentic. (Crypto checksums could be used, although they create a new set

of vulnerabilities.) Sooner or later someone will indeed post a bogus message to the entire RISKS group, with fake authorship and bypassing my moderation; I will then have to point out that I stated in RISKS-5.4 (and earlier, as well) that it can of course be done. (I have tried to use TOPS-20 as sensibly as possible to make such immoderation nontrivial, but I cannot seal off that possibility altogether.) Besides, I would like to believe that the RISKS community consists mostly of socially conscious and thoughtful individuals, interested in learning and growing in awareness.

Careful RISKS readers must by now realize that I am probably the last person in the world who would say that something is really secure -- I know that NOTHING is, including the interposition (or imposition?) of RISKS moderation. I simply must rely on your sensitivity not to mount attacks. We will soon have to switch to a UNIX system on a Sun workstation as the RISKS source, and at that point I would otherwise have to abandon all hope of moderation.

PGN

A Passive-Aggressive User Interface -- U.Iowa telephone tidbits

<Peter G. Neumann <Neumann@csl.sri.com> [Really-From Ray Ford]>
Wed 24 Jun 87 00:17:17-PDT

(From the University of Iowa "fyi", 12 June 1987, p.2, in its entirety. Contributed by Ray Ford, whose interspersals are in square brackets.)

Telephone tidbits

[The Passive Aspect:]

No answer

University telephone users should be advised that when a University telephone has been programmed for call forward busy/no answer, the caller will hear three rings before the unanswered phone switches to its forwarded number. If that number is busy, however, the caller will not get a busy signal but will continue to hear the ringing signal. This is a problem with the software for the system, according to the office of telecommunications, for which there is no apparent solution.

[The Aggressive Aspect:]

Nothing in common

The full-feature electronic telephones called D-Terms now in use on the University system are not compatible with Northwestern Bell or any other telephone system. Serious mishap, including explosion and fire, can occur if these telephones are connected to the wrong system.

Bogus ROOT domain server on ARPAnet

Robert Lenoil <@EDDIE.MIT.EDU:LENOIL@DEEP-THOUGHT.MIT.EDU>
Fri 19 Jun 87 15:31:12-EDT

Here is an interesting example of how a malicious host could cause considerable interruption to the ARPANET:

> Subject: Bogus ROOT domain server on ARPAnet [PGN Excerpting Service]
> Date: Mon, 08 Jun 87 22:40:46 -0500
> From: Paul Richards <richards%shangrila.cs.uiuc.edu@a.cs.uiuc.edu>
>
> Tonight, we had what I'd call a major failure on the ARPA domain name system. A system at NORTHWESTERN.ARPA, [10.4.0.94], started advertising itself as a root domain name server, with the consequences that we stopped being able to locate any domain names at all....
>
> Paul Richards University of Illinois at Urbaba-Champaign; Computer Science
> richards@b.cs.uiuc.edu, +217 333-3536

Printer raises utility false alarm

"A. Harry Williams" <HARRY%MARIST.BITNET@wiscvm.wisc.edu>
Mon, 22 Jun 87 10:01:02 EDT

Last week the local utility company was training the Customer Support Reps (CSR) on the new procedures for emergency outages, such as during a storm. There were several people from different areas in the company, all at the main site. One of the screens on the computer terminal used for handling the emergency problems calls for the name of a printer to print the report. One of the people involved could only remember the name of the printer in the main operations for the company. Needless to say, there were several hurried phones calls after a utility company crew and police arrived at the "scene of the downed power lines" to find no problem existing. Fortunately, the name of the CSR is on report, so they were able to track down the person that way, and find out the false alarm. A little while later the operations room called back and asked if they had sent out a gas crew an hour before.

[New VAX UNIX file system disk purge runs amok]

<Mike.Accetta@q.cs.cmu.edu>
22 Jun 87 13:03:20 EDT

We experienced serious file system losses on many of the VAX UNIX systems this weekend beginning early in the morning on Saturday 6/20. At that time, a new system file which controls the disk purge operation was distributed and failed on all of the VAX systems which received it. On all but three machines this operation was aborted after removing a substantial number of its system files but before any private files were affected. These machines were returned to service upon restoration of their system files during the weekend. The following machines:

SPEECH2.CS.CMU.EDU SAM.CS.CMU.EDU ME.RI.CMU.EDU

each also lost a large part of one of their private file partitions. These file partitions are in the process of being restored from tape backups and the machines should be back in at least limited service by 1400 Monday, 6/22.

Normally, the particular disk purge operation in question would have recursively removed all files in /usr/preserve that were more than a week old. However, on Saturday morning the mode of failure resulted in the attempted recursive removal beginning at / of all files which were more than a week old on each affected system.

Machines with (to our knowledge) only system files removed were:

PH1.SPEECH.CS.CMU.EDU FAS.RI.CMU.EDU GNOME.CS.CMU.EDU
G.CS.CMU.EDU THEORY.CS.CMU.EDU UNH.CS.CMU.EDU
ROVER.RI.CMU.EDU ISL1.RI.CMU.EDU IUS1.CS.CMU.EDU
IUS2.CS.CMU.EDU SPEECH1.CS.CMU.EDU CIVE.RI.CMU.EDU

Finally, a number of the VAX workstations were also affected. Problems have been corrected and all system files restored on:

LAB.AGORA EDJ.ARCHONS EMC.CS EP.FAC
MRT.MACH PIE5.MACH A.NL AMADEUS.PRODIGY
DRAKON.RESDOC F.SPEECH G.SPEECH Y.SPEECH
SPEECH3 NDIFF.VLSI D.SPEECH

Some workstations where a problem is suspected were inaccessible and have not yet been checked and/or corrected. We will attempt to track down and if necessary correct problems with these systems on Monday. You may also contact the Operator at x2607 to report a problem if your machine appears to be in this category,

So far as we know, no private files on any workstation examined so far were removed and over all only VAX mainframe and workstation systems were affected. At this point, while we know what went wrong and where, we still do not completely know why.

We do apologize for any inconvenience this failure has caused.

Search RISKS using swish-e

THE RISKS DIGEST

Forum on Risks to the Public in Computers and Related Systems

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

Volume 5: Issue 4

Wednesday, 24 June 1987

Contents

Immoderation and Nonmoderation

Peter G. Neumann <Neumann@csl.sri.com>
Tue 23 Jun 87 16:53:12-PDT

A few of you have received a UUCP message through "cbosgd" that intended to demonstrate that systems are not really very secure and that it is easy to bypass moderation on supposedly moderated news groups. (The message in question was written as a response to someone who thought that this might be difficult!) The existence of that message should not surprise any readers of RISKS, who by now have no trouble grasping the fact that there is no such thing as complete security. However, the message was sent not through RISKS@CSL but through one of our innumerable redistribution points (and thus was received by only a very small fraction of all RISKS readers). The possibility of doing that should not be a surprise, particularly in that most local redistribution centers have been explicitly set up to be automatic forwarders rather than requiring manual intervention.

A long time ago Dave Parnas objected to having his position papers on Star Wars serialized in Soft-Eng@MIT-XX and circulated via netmail, partly because there are no guarantees that the received message was actually authentic. (Crypto checksums could be used, although they create a new set

of vulnerabilities.) Sooner or later someone will indeed post a bogus message to the entire RISKS group, with fake authorship and bypassing my moderation; I will then have to point out that I stated in RISKS-5.4 (and earlier, as well) that it can of course be done. (I have tried to use TOPS-20 as sensibly as possible to make such immoderation nontrivial, but I cannot seal off that possibility altogether.) Besides, I would like to believe that the RISKS community consists mostly of socially conscious and thoughtful individuals, interested in learning and growing in awareness.

Careful RISKS readers must by now realize that I am probably the last person in the world who would say that something is really secure -- I know that NOTHING is, including the interposition (or imposition?) of RISKS moderation. I simply must rely on your sensitivity not to mount attacks. We will soon have to switch to a UNIX system on a Sun workstation as the RISKS source, and at that point I would otherwise have to abandon all hope of moderation.

PGN

A Passive-Aggressive User Interface -- U.Iowa telephone tidbits

<Peter G. Neumann <Neumann@csl.sri.com> [Really-From Ray Ford]>
Wed 24 Jun 87 00:17:17-PDT

(From the University of Iowa "fyi", 12 June 1987, p.2, in its entirety. Contributed by Ray Ford, whose interspersals are in square brackets.)

Telephone tidbits

[The Passive Aspect:]

No answer

University telephone users should be advised that when a University telephone has been programmed for call forward busy/no answer, the caller will hear three rings before the unanswered phone switches to its forwarded number. If that number is busy, however, the caller will not get a busy signal but will continue to hear the ringing signal. This is a problem with the software for the system, according to the office of telecommunications, for which there is no apparent solution.

[The Aggressive Aspect:]

Nothing in common

The full-feature electronic telephones called D-Terms now in use on the University system are not compatible with Northwestern Bell or any other telephone system. Serious mishap, including explosion and fire, can occur if these telephones are connected to the wrong system.

Bogus ROOT domain server on ARPAnet

Robert Lenoil <@EDDIE.MIT.EDU:LENOIL@DEEP-THOUGHT.MIT.EDU>
Fri 19 Jun 87 15:31:12-EDT

Here is an interesting example of how a malicious host could cause considerable interruption to the ARPANET:

> Subject: Bogus ROOT domain server on ARPAnet [PGN Excerpting Service]
> Date: Mon, 08 Jun 87 22:40:46 -0500
> From: Paul Richards <richards%shangrila.cs.uiuc.edu@a.cs.uiuc.edu>
>
> Tonight, we had what I'd call a major failure on the ARPA domain name system. A system at NORTHWESTERN.ARPA, [10.4.0.94], started advertising itself as a root domain name server, with the consequences that we stopped being able to locate any domain names at all....
>
> Paul Richards University of Illinois at Urbaba-Champaign; Computer Science
> richards@b.cs.uiuc.edu, +217 333-3536

Printer raises utility false alarm

"A. Harry Williams" <HARRY%MARIST.BITNET@wiscvm.wisc.edu>
Mon, 22 Jun 87 10:01:02 EDT

Last week the local utility company was training the Customer Support Reps (CSR) on the new procedures for emergency outages, such as during a storm. There were several people from different areas in the company, all at the main site. One of the screens on the computer terminal used for handling the emergency problems calls for the name of a printer to print the report. One of the people involved could only remember the name of the printer in the main operations for the company. Needless to say, there were several hurried phones calls after a utility company crew and police arrived at the "scene of the downed power lines" to find no problem existing. Fortunately, the name of the CSR is on report, so they were able to track down the person that way, and find out the false alarm. A little while later the operations room called back and asked if they had sent out a gas crew an hour before.

[New VAX UNIX file system disk purge runs amok]

<Mike.Accetta@q.cs.cmu.edu>
22 Jun 87 13:03:20 EDT

We experienced serious file system losses on many of the VAX UNIX systems this weekend beginning early in the morning on Saturday 6/20. At that time, a new system file which controls the disk purge operation was distributed and failed on all of the VAX systems which received it. On all but three machines this operation was aborted after removing a substantial number of its system files but before any private files were affected. These machines were returned to service upon restoration of their system files during the weekend. The following machines:

SPEECH2.CS.CMU.EDU SAM.CS.CMU.EDU ME.RI.CMU.EDU

each also lost a large part of one of their private file partitions. These file partitions are in the process of being restored from tape backups and the machines should be back in at least limited service by 1400 Monday, 6/22.

Normally, the particular disk purge operation in question would have recursively removed all files in /usr/preserve that were more than a week old. However, on Saturday morning the mode of failure resulted in the attempted recursive removal beginning at / of all files which were more than a week old on each affected system.

Machines with (to our knowledge) only system files removed were:

PH1.SPEECH.CS.CMU.EDU FAS.RI.CMU.EDU GNOME.CS.CMU.EDU
G.CS.CMU.EDU THEORY.CS.CMU.EDU UNH.CS.CMU.EDU
ROVER.RI.CMU.EDU ISL1.RI.CMU.EDU IUS1.CS.CMU.EDU
IUS2.CS.CMU.EDU SPEECH1.CS.CMU.EDU CIVE.RI.CMU.EDU

Finally, a number of the VAX workstations were also affected. Problems have been corrected and all system files restored on:

LAB.AGORA EDJ.ARCHONS EMC.CS EP.FAC
MRT.MACH PIE5.MACH A.NL AMADEUS.PRODIGY
DRAKON.RESDOC F.SPEECH G.SPEECH Y.SPEECH
SPEECH3 NDIFF.VLSI D.SPEECH

Some workstations where a problem is suspected were inaccessible and have not yet been checked and/or corrected. We will attempt to track down and if necessary correct problems with these systems on Monday. You may also contact the Operator at x2607 to report a problem if your machine appears to be in this category,

So far as we know, no private files on any workstation examined so far were removed and over all only VAX mainframe and workstation systems were affected. At this point, while we know what went wrong and where, we still do not completely know why.

We do apologize for any inconvenience this failure has caused.

Search RISKS using swish-e

THE RISKS DIGEST

Forum on Risks to the Public in Computers and Related Systems

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

Index to Volume 4

Saturday, 6 June 1987

- Re:airplanes and risks, Risks 3.89 (Udo Voges)

Volume 4 Issue 7 (7 Nov 86)

- Risks of RISKS (PGN)
- Details on the British Air Traffic Control computer outage (from Herb Hecht)
- Re: UK computer security audit (Robert Stroud)
- USS Liberty (Matthew P Wiener)
- Grassroots sneak attack on NSA (Matthew P Wiener)
- A variation of the Stanford breakin method (Arno Diehl)
- Re: Subject: Computers and Medical Charts (Roy Smith)
- DDN Net breakdown (?) on 6 Nov 86? (Will Martin)
- Re: Linguistic decay (Matthew P Wiener)
- Mechanical Aids to Writing (Earl Boebert)

Volume 4 Issue 8 (9 Nov 86)

- Brazilian laws require proof of voting. People NEED those cards. (Scot E. Wilcoxon)
- Grassroots sneak attack on NSA (Herb Lin, Matthew P Wiener)
- Ethernet Security Risks (Phil Ngai)
- Perfection (Herb Lin)
- Information replacing knowledge (Daniel G. Rabe)
- Word Processors / The Future of English (Stephen Page)
- Copyrights; passwords; medical information (Matthew P Wiener)

Volume 4 Issue 9 (10 Nov 86)

- Risk of aging (Lee F. Breisacher)
- Re: UK computer security audit (Henry Spencer)
- Lost files (Norman Yusol)
- Canard!! [Looping Mailers] (Lindsay F. Marshall)
- Friend-foe identification (Henry Spencer)
- Micros in Car Engines (Jed Sutherland)
- Information replacing knowledge (Bard Bloom, Herb Lin, Jerry Saltzer)
- Spelling becoming obsolete? (Ted Lee)
- They almost got me! [A motor-vehicle database saga] (Mark Hittinger)

Volume 4 Issue 10 (12 Nov 86)

- Extreme computer risks in British business (Lindsay F. Marshall)
- Alabama election snafu caused by programmer (PGN)
- Looping mailer strikes again (Brian Reid, Nancy Leveson)
- Lost files on Bitnet (Niall Mansfield)
- VOA car testing (Bill Janssen)
- Re: Aftermath of the Big Bang (apology) (Robert Stroud)
- Re: The Future of English (T. H. Crowley [both of them])
- Word-processors Not a Risk (Ralph Johnson)

Volume 4 Issue 11 (14 Nov 86)

- Computers don't kill people, people kill people (Howard Israel)
- Open microphone in the sky (Bob Parnass)
- Computerized Voting in Texas (Jerry Leichter)
- Problems with HNN (Alan Wexelblat)
- Post-hacker-era computer crime (Talk by Sandy Sherizen)
- Re: They almost got me! [A motor-vehicle database saga] (Doug Hardie)

THE RISKS DIGEST

Forum On Risks To The Public In Computers And Related Systems

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

Search RISKS using swish-e

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

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

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

Feeds

RSS 1.0 (full text)

RSS 2.0 (full text)

ATOM (full text)

RDF feed

WAP (latest issue)

Simplified (latest issue)

Smartphone (latest issue)
Under Development!!

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

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

Selectors for locating a particular issue from a volume

Volume number: Volume Issue Number: Issue

Get Specific Issue

Volume Index

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

Index to the RISKS Digest

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

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

Search RISKS using swish-e

THE RISKS DIGEST

Forum on Risks to the Public in Computers and Related Systems

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

Index to Volume 6

Tuesday, 31 May 1988

Full Body Scan and pat down in progress

You were warned....

Search RISKS using swish-e

THE RISKS DIGEST

Forum on Risks to the Public in Computers and Related Systems

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

Volume 5: Issue 5

Friday, 26 June 1987

Contents

Re: Immoderation and Nonmoderation

Joe Buck <jbuck@epimass.epi.com>
25 Jun 87 21:01:55 GMT

>From: Peter G. Neumann <Neumann@csl.sri.com>
>A few of you have received a UUCP message through "cbosgd" that intended to
>demonstrate that systems are not really very secure and that it is easy to
>bypass moderation on supposedly moderated news groups... However, the message
>was sent not through RISKS@CSL but through one of our innumerable
>redistribution points (and thus was received by only a very small fraction of
>all RISKS readers).

Wrong.

The parochialism of our Arpanet brethren never ceases to amaze me. The vast

majority of RISKS readers are on Usenet. Usenet is far larger than the Internet, Bitnet, etc, and almost every Usenet site that receives RISKS (alias comp.risks). UUCP is just a transport mechanism (Usenet != UUCP-net); many ARPA Internet sites now receive their mailing lists Usenet-style using the nntp system. The forged article in question travelled to every Usenet site (including those Internet sites that use nntp). Usenet does not use mail, but rather a flooding mechanism; every site sends it to all their downstream links until everyone has the article. If many people didn't see it, that's because several people issued "cancel" messages to make it disappear. (These messages were forged also). -- - Joe Buck jbuck@epimass.EPI.COM
{seismo,ucbvax,sun,decwrl,<smart-site>}!epimass.epi.com!jbuck
Old arpa mailers: jbuck%epimass.EPI.COM@seismo.css.gov

[Thanks for the comments. I maintain a large list of direct addresses to redistribution centers (and a few individuals) on ARPANET, MILNET, CSNET, BITNET, etcNET -- with many indirections -- and those readers simply did not get the message in question. They did not miss anything.

By the way, "forged" is not quite right. On the basis of the dialogue, I conclude that the message was REALLY-FROM "apc". It was just a public misuse of a useful but totally unsound facility -- subject to loss of privacy at each forwarding, loss of data integrity on any message, and complete denial of service if a message is cancelled along the way. (Use of the RISKS banner and standard DIGEST format would have constituted forgery. It is interesting to contrast this with Piet Beertema's "Chernenko@MOSKVAX" -- Software Engineering Notes, vol 9, no 4, July 1984.) PGN]

[From: cmcl2!phri!roy@seismo.CSS.GOV (Roy Smith)
Organization: Public Health Research Inst. (NY, NY)
... In its alter-ego, RISKS appears on the wild-and-wooly Usenet as the newsgroup comp.risks. Netnews has lots of advantages over mailing lists but security isn't one of them.

... suffice it to say that ["apc" 's abuse of RISKS] was stupid and childish, and the tail-end of some totally absurd argument that has been going on for weeks all around the net. Roy Smith, {allegra,cmcl2,philabs}!phri!roy]
[Note: There are advantages of unmoderated newsgroups and advantages of moderated newsgroups. I try to maintain a relatively open policy (subject to the masthead guidelines); at least the "official" version of RISKS will remain moderated. PGN]

"Computer woes hit air traffic" [Boston Globe, Monday, June 15, 1987]

Alex Jenkins <atj@mirror.TMC.COM>
Wed, 24 Jun 87 10:14:47 edt

Boston (AP) - "A computer problem that blanked the radar screens of air traffic controllers from New England to the Great Lakes for six minutes delayed flights at Logan International Airport, but posed no hazard, an official said. When the outage occurred Saturday afternoon, planes immediately were ordered to fly more slowly and at greater distances from

each other, according to Mike Ciccarelli, a spokesman for the Federal Aviation Administration. He said some flights were rerouted and planes scheduled to fly into New England were ordered to remain on the ground. 'There were delays of incoming flights, naturally, because if they wanted to leave Newark, for example, they couldn't,' Ciccarelli said. He said Logan has a separate monitoring system which kept the controllers in radar contract(sic) with flying aircraft."

[The SF Chron reported this on 21 Jun 87. After quoting Ciccarelli that there was no hazard for air travelers, it went on to say, ``... although a controller who asked not to be identified described the situation as "very dangerous".'' Increasingly the air traffic control operations are coming under scrutiny. Oprah Winfrey had a fine show the other day. PGN]

Alex T. Jenkins, Mirror Systems, Cambridge Massachusetts atj@mirror.TMC.COM

BBC documentary filming causes Library of Congress computer crashes

Mark Brader <msb@sq.com>
Thu, 25 Jun 87 22:21:20 EDT

The following article was in comp.misc on Usenet. It was posted as a followup to the "exploding computers" articles [RISKS-5.6], but it is really a separate topic and an interesting hazard. [Forwarded to Risks by Mark Brader]

From: howard@COS.COM (Howard C. Berkowitz)
Message-ID: <312@cos.COM>
Date: 4 Jun 87 13:44:18 GMT
Organization: Corporation for Open Systems, McLean, VA

In the late '70's, I worked at the Library of Congress. We had IBM and Amdahl mainframes with STC tape drives as our main data base machines. Given the role of the world's largest library, our computer room received considerable attention.

The British Broadcasting Corporation was given access to much of the Library, to film a documentary. We found that some major system crashes began to happen when they were in the computer room. We thought it might be their video equipment, floods, etc., but could not find the cause.

The symptom was clear: periodically, ALL of our tape drives would simultaneously stop, rewind, and unload, no matter what they were doing. The operating system could not deal with such simultaneous events, and would crash.

It turned out to be an intermittent event: most BBC work was film or video, but they occasionally took still photographs. When their electronic flash pointed at the front of the tape drives, the short burst of light was reflected into the photoelectric end-of-tape sensors of each tape drive, causing EVERYTHING to simultaneously sense (erroneously) end-of-tape.

Running out of gas could be hazardous!

Steve McLafferty <harvard!munsell!ssm@seismo.CSS.GOV>
24 Jun 87 17:22:12 GMT

Several months ago I posted an article to comp.risks (RISKS 4.46) about the electronic steering in the Pontiac Pursuit project car. All four wheels on the car can be steered, and the force required to turn the wheels comes from DC powered motors that are computer controlled. There is no direct physical connection from the steering wheel to any of the wheels. This article triggered a small debate in RISKS over the use of electronics in automobiles.

The June 22, 1987 issue of AUTOWEEK contains a follow up story on the Pursuit. They took a test drive of the car, fortunately at a closed race track rather than on the highway. During the test drive, the car ran out of gas. When the engine stopped, so did the 24-volt alternators which supply power to the steering system. The steering failed, and the car ran off the track! Apparently there was no battery backup for the 24-volt system.

NASA Safety Reporting System

Eugene Miya N. <eugene@ames-pioneer.arpa>
25 Jun 1987 1708-PDT (Thursday)

NASA NEWS
NASA ESTABLISHES SAFETY REPORTING SYSTEM

NASA has established a voluntary, confidential safety reporting system for its 100,000 employees and contractor personnel to alert NASA management of safety concerns.

The new reporting system supplements existing safety reporting procedures and, initially, will focus on safety concerns associated with NASA's Space Transportation System, more familiarly known as the Space Shuttle program. The new system is being established as a result of the Shuttle Challenger accident.

The NASA Safety Reporting System (NSRS) will encourage employees to supplement existing safety reporting procedures by completing and submitting an NSRS confidential report form to Battelle Memorial Institute's Columbus Division, Columbus, Ohio. Battelle Institute is under contract to NASA to develop and administer the NSRS for NASA Headquarters' Safety Division.

Use of the NSRS report form will provide anonymity to the maximum extent possible within the law for individuals disclosing their safety concerns. The form will contain a section at the top for individuals to include their names, addresses and telephone numbers.

Upon receipt of the report form, the Battelle NSRS team will remove this top section unless team members determine that additional data would be useful. If so, the team will contact the sender for the needed information and then remove, stamp and return the top section to the sender as proof that the sender has successfully filed a NSRS report. No record will be maintained of reporting individual's identities.

Battelle NSRS and NASA specialists then will determine whether the reported concern is of a critical nature requiring immediate action.

The Battelle NSRS team will summarize all reported concerns, store the deidentified data in a computerized data management system and forward summaries to the NASA Headquarters Safety Division for further analyses in cooperation with a technical advisory group.

The Safety Division and technical advisory group also will determine what corrective action should be taken and track the resolution of these recommendations.

= =

NASA NEWS Release 87-91
By David W. Garrett, Headquarters, Washington, D.C.
Reprinted with permission for electronic distribution

= =

A comment on anonymous reporting systems: the AEC (then ERDA, then NRC and the DOE) have had such a reporting system for years. Every nuclear facility in the country has a special phone with a direct line to Washington DC, but it is rarely used and is poorly maintained. Many "employee suggestion" programs have not worked for various fears. Some have supposedly worked in Japan. I have noted no such systems on computers since E-mail always has had return addresses. What can we do to get people to use such systems?

--eugene miya, NASA Ames Research Center

EGP madness

David Chase <rbbb@rice.edu>
Thu, 25 Jun 87 21:30:49 CDT

Recently Rice University was the victim of a little Internet EGP madness. I will try to give a coherent summary, though we still don't know how it came about.

Sometime in the evening of June 23, Libra.Rice.EDU, Rice's ARPANET gateway, started receiving packets destined for "css-ether" (Center for Seismic Studies Ethernet, including the machine "seismo.css.gov") and "univ-ariz" (University of Arizona Ethernet). Libra.Rice.EDU (10.4.0.62, 128.42.1.64) is an LSI-11 running Dave Mills's "Fuzzball" software. Because of the address space limitations of the PDP-11 architecture, Libra occasionally runs out of room in its routing table. We suspected that such an event might have confused Libra's EGP to the point where it sent out bogus routing updates.

A quick check showed that Libra still knew the correct routes to css-ether and univ-ariz. Still, we were worried because the tables were in fact full, so we took the gateway down for about an hour around Midnight and restarted it with expanded tables. We then did our best to determine that we were not advertising ourselves as a gateway to either network.

After midnight, we continued to receive packets destined for seismo, with

sustained traffic about 4 times higher than normal. We called BBN the following morning (June 24), and learned that bbnnet2-arpanet-gw, one of the three "public" EGP-speaking core gateways, continued to list us as the gateway, with metric 2, for css-ether and univ-ariz. The other two core gateways had the correct routes, and BBN confirmed that Libra was advertising only legitimate routes. The erroneous traffic fell off markedly when bbnnet2-arpanet-gw was rebooted that afternoon, but occasional misdirected packets persisted until late this morning (June 25).

The same evening that Libra's gateway tables filled up, BBN had loaded "new test software" into that gateway machine, so there is no clear smoking gun here.

This story has a "happy ending", because our Fuzzball stayed up the whole time and dutifully forwarded packets and sent ICMP squawks to the offending machines.

Now, the bad part. At least 78 hosts were fooled (that is, 78 hosts were fooled in some given hour, because the log file wrapped around about once per hour), including machines from nets 8, 10, 18, 26, 128.{8,32,41,45,59,83,84,95,102,103,104,105,115,121}, 192.1.2, 192.5.{25,58} and 192.12.{31,33,119,206,221}. We don't know the cause of this problem, but it does seem like a bit of a security hole. We could easily have wiretapped all the traffic for seismo.css.gov, or even substituted our own more "interesting" packets. Thus we were particularly amused to find traffic from Milnet hosts (11 of them) passing through us.

David Chase and Paul Milazzo
Department of Computer Science, Rice University

Re: EGP madness

<Mills@UDEL.EDU>
Fri, 26 Jun 87 0:24:03 EDT

Interesting. During the time you report loyal fuzzball linkabit-gw was having exactly the same problem, mounds and mounds of traffic sloshing in and getting dutifully redirected. However, another fuzzball dcn-gw was having no such prolem. All squawk the same EGP code as yours and linkabit-gw at least has the same table-space problem as yours.

There is a clue in the clock-synchronization system that you may have noticed. I began seeing frequent clock resets, with measured roundtrip times one hop away as the ARPANET flies reaching twenty seconds or more (!?). When I checked the INOC for core gateway routes, I found the directly-connected macomnet client of linkabit-gw as reachable via purdue-gw! Something was badly wrong in the core system.

Prompted by a note from Joe Weening at SU, I found a wee bug in the fuzzball EGP code that would, under bizarre conditions I hastily add, result in a nonsense address in a redirect message sent by the fuzz. The bog is now

fixed in linkabit-gw and dcn-gw. I can't see how the bog would affect the slosh you an I saw over the last few days anyway, but it might under unlikely conditions result in a j-random host, having mistakenly been redirected to your gateway, not being redirected back to the proper gateway.

Re: EGP madness

<Mills@UDEL.EDU>
Fri, 26 Jun 87 0:28:41 EDT

I forgot to add that table overflow will not affect what you send the core, only what you can reach. If the table does overflow, the net(s) lost will appear unreachable. I'm working on that. Also, I saw evidence that the core tables were being corrupted with martians (net 112?!) that reached back to touch us in the swamps. I also saw broadcasts (sic) coming from a 128.205 hosts landing at linkabit-gw, truly a martian who lost his compass.

FCC Information Tax -- Risks of Networking

<"IMS/Steve Schultz" <steve@afsc-bmo.arpa> [info-law]>
24 Jun 87 11:49:00 PST

From: hadeishi@husc4.HARVARD.EDU (mitsuharu hadeishi)
Subject: ATTENTION ALL MICRO USERS!!! FCC INFORMATION TAX AHEAD!!
Date: 12 Jun 87 15:13:37 GMT

A terrible piece of news I just read about in the New York Times this morning. The FCC just voted 4-0 to impose a $4.50 - $5.50 an HOUR tax on people who are using the phone system to transmit information across state lines. This INCLUDES anyone hooking up to a network, not just people dialing out of state!! I suppose people dialing into a system with access to Arpanet or even USENET might be charged this tax; the information services (Compuserve, etc.) are slated to be charged this tax as of January 1. This is an outrageous tax which would squelch the burgeoning telecommunications industry, and is totally unjustified. I would urge people to write letters to their Congressman to protest this unfair and exorbitant "information tax" which is based on superstition and lack of understanding of the telecommunications industry.

-Mitsu
John Langbein

Search RISKS using swish-e

THE RISKS DIGEST

Forum on Risks to the Public in Computers and Related Systems

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

Volume 5: Issue 6

Friday, 26 June 1987

Contents

Hardware vs Software Battles (from Usenet)

Mark Brader <msb@sq.com>
Thu, 25 Jun 87 22:18:40 EDT

[I have selected the following articles from a long discussion in the
Usenet newsgroup comp.misc. My interpolations are marked like this.
I have deleted some header lines, some text, and all signatures.
--msb (Mark Brader)]

> [TNX. Although Usenet readers may already have been saturated with this material, the VAST MINORITY of remaining readers in the rest of the net world also deserves to see it. PGN]

What the world needs now

Jonathan D. <trudel@topaz.rutgers.edu>
18 May 87 19:01:57 GMT

... is a piece of software that actually makes a computer blow up just like in the movies. This is long overdue. "Lay" people are extremely disappointed when a program or system grinds/wheezes to a halt with some wimpy message like "B037X: USER ERROR IN GAPX TABLE" or "CATASTROPHIC SYSTEM FAILURE: BUFFER OVERFLOW INDICATOR OVERFLOW" or "Bus error - core dumped". They want to see explosions! Paper spewing out from wherever paper spews out from! And gicky fluid oozing out of the machinery as the entire machine room collapses onto itself because someone either forgot to put a %*&#*$#&@ in column 92 or asked the computer an impossible question like "What's the meaning of life?", "Why?", "CAN you get there from here?", "Calculate pi to the last digit" [THAT'S NOT A QUESTION!], or "Where's the bathroom?" That's a worthy goal for computer technologists everywhere. Forget artificial intelligence! Forget relational databases! Forget distributed network architecture proposal interface protocols! Forget documentation! Forget associative memory! Let's make computers explode in our lifetime!!!

requiring hardware repairs? Like this... --msb]

From: rick@oresoft.UUCP (Rick Lahrson)
Message-ID: <37@oresoft.UUCP>
Date: Mon, 25-May-87 02:52:46 EDT
Organization: Oregon Software, Portland OR

A small step was taken toward this end back in the early sixties, in IBM's System/360 model 30 CE school. Seems one of the better students had time enough to pore over the schematics and discover which cores (remember core memory?) were located just beneath the overtemp sensor. He wrote a small program that did nothing but abuse those particular cores by writing ones and zeroes alternately to them, until they heated up, and the temperature sensor shut down the machine.

First, of course, the program printed out "Programmed Power Down" on the console. Caused a lot of bewilderment among the students and instructors. Especially since the big feature being touted about the S/360 was that it was so oriented to multiprogramming that it didn't even have a HALT instruction.

arate discussion in misc.misc, but what the heck, it fits in nicely here), pointing out that a number of modern computers have a software-handled OFF switch, and have to have their plugs pulled when they get totally stuck. These articles were then nicely topped by this one: --msb]

From: bill@sigma.UUCP (WIlliam Swan)
Message-ID: <1261@sigma.UUCP>
Date: 19 Jun 87 16:35:12 GMT
Organization: Summation Inc, Kirkland WA

Some years ago I worked on a battery-powered instrument (it would run 24 to 48 hours on batteries) in which the project manager insisted that the OFF switch should be an interrupt to the CPU, which would then power itself down.

You guessed it.. the uP derailed and the only ways to get it back were:
1. Open the instrument up and yank the battery leads, or
2. Pull it off the charger and wait a day or two.

Fortunately (:-) it never made it to market.

Imagine being the person who set it off by accident! --msb]

From: kmd@sdcsmb.UUCP (Karen M. Davis)
Message-ID: <424@sdcsmb.UUCP>
Date: Fri, 22-May-87 11:47:38 EDT
Organization: System Development Corporation, Santa Monica CA

Um.... many computers built for military applications contain a "trap door" that can be reached by an assembly sequence that will direct the transformer or power supply *input* onto the motherboard. Manufacturers of this type of computer include HP and Litton. This "feature" is supposed to be used to destroy your computer as the installation is being overrun by the enemy. Since most of these suckers use large DC generators as input to the transformers/power supplies, you can imagine the fireworks that occur when this stuff reaches all those cute little ICs. ;-)

It was supposed to leave the attackers with molten sludge.

drives and "halt and catch fire" instructions, but the following ones seemed sufficiently well described to include here. Some relate to deliberate actions, but in every case there is the question, "what if this happened by accident?" --msb]

From: socha@drivax.UUCP (Henri J. Socha (x6251))
Message-ID: <1827@drivax.UUCP>
Date: 11 Jun 87 18:59:22 GMT
Organization: Digital Research, Monterey

The following story was related to me by employees of I.P. Sharp Associates (IPS). They, with Scientific Time Sharing Corp. (STSC) wrote APL for IBM back in the early days.

It seems that there started to be competitors to IPS/STSC's APL system. These companies would usually use IBMs APL (written by IPS/STSC) on their large IBM mainframes. Sometimes they would add extra bulletproofing so that APL would not bomb, get better performance, etc.

Now, IPS/STSC really knew APL (and the IBM implementation) very well.
In fact, an employee living in Palo Alto would debug/enhance the
production on-line APL system from his home!

There were people across North America and in Europe (at that time) using
this single mainframe (360/158 I think). The computer was in Toronto Canada.

Anyway, a competitor named Manhattan APL (I think) called up IPS and said
they were about to come online and if IPS wanted to, they could test
the system. Manhattan said they had filled in all the holes and the system
was unbreakable.

Manhattan APL came online for their customers about 2 months late.
It seems that some of their disk drives had thrashed themselves to death.

Stuart D. Gathman <stuart@bms-at.UUCP>
28 May 87 19:02:14 GMT

I inadvertently wrote a BASIC program on an HP2000 at George Mason University
that blew up the disk drive. It was an 8 player real time space war game.
The problem was that all interprocess communication had to take place via
disk. I used the documented LOCK function for serialization. It seems that
this function loaded a special OS overlay whenever invoked and reloaded
the file I/O overlay directly afterward. With 8 programs doing this
as fast as possible, the disk would die.

The problem was solved by using an undocumented feature of the scheduler.
A process was always assigned 1 sec of CPU following completion of a wait
for terminal I/O. This allowed serialization with careful coding while
not using the LOCK overlay.

BTW, an IBM PC program can blow up the monitor and video cards by programming
nasty parameters into the video controller chip.

Peter DaSilva <peter@sugar.UUCP>
10 Jun 87 13:08:32 GMT

The CompuColor 2 personal computer of about the 1978-80 era could be made
to fry itself from BASIC. A simple FOR loop outputting 1-255 into a certain
I/O address (it's Z-80 based) caused the screen to blank in an entertaining
fashion, followed by the smell of smoke. You had to pull the plug at the
wall to get it to stop. I was totally amazed. Just think of the possibilities.
I don't know exactly what was going on, but I suspect that they had too much
trust in software and used the CPU to control such things as the power supply
so they could save $5 worth of chips.

The Sentinel <sentinel@killer.UUCP>
Wed, 20-May-87 20:30:14 EDT

When I was in high school, we had several SWTPC 6800 machines, of slightly post-Altair vintage. They had 32k of RAM (a lot at the time), 5-1/4" single density drives that held around 90k, a CP/M-like operating system, and you had to boot them by calling the disk boot rom from the monitor.

Anyway, I saw demonstrated (not with the school's permission, as you can probably guess) a program called "DEATH" which did a number of destructive things including stepping the drives out of range and apparently using this opcode you mention. I remember the main board going in for service after that and coming back with lots of new chips. I never knew how a program could do this until now...

(Don't take everything I said as absolute truth... my memory is a bit fuzzy... I do distinctly remember the computer being fried by that program, though. And no, I was not the one who did that... I was only a spectator)

On another note, some of the earlier Commodore PET's had a register in their video controller that set the number of scan lines (or something like that). On some of them, you could tweak this register to get a better looking screen display. On others, doing so would toast the video circuitry. While this is not strictly in the "exploding computer" category, in the PETs the monitor WAS in the same case, so it has the same effect on the poor guy who watches it happen :-)

David Phillip Oster <oster@dewey.soe.berkeley.edu>
Thu, 21-May-87 13:53:35 EDT

A few years back, PC magazine and PC World published claims that it was possible to program the video controller chip in the CGA (Computer Graphice Adapter) video adapter board so that an ordinary color monitor's flyback transformer would overheat and catch fire. Has anybody done this? Is it included in anyone's copy detection? Anyone's error handler?

It should be real simple to do. That chip gives you pretty good control over the video waveform, so you ought to be able to play with the timing of the horizontal sync pulse, (which, as I remember, was the way the trick was done.) has anybody extened these techniques to the more sophisticated EGA (Extended Graphics), and PGA (Professional Graphics).

[End of collection forwarded to Risks by Mark Brader--msb]

Report problems with the web pages to the maintainer

Search RISKS using swish-e

THE RISKS DIGEST

Forum on Risks to the Public in Computers and Related Systems

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

Volume 5: Issue 7

Sunday, 5 July 1987

Contents

Actual stock price change fails sanity check

Mark Brader <msb@sq.com>
Mon, 29 Jun 87 13:00:34 EDT

In the 1880's the Canadian Pacific Railway wanted a line between Montreal and Toronto but could neither afford to build one nor to buy out an existing railway. So what they did was to take a perpetual lease on an existing railway, the Ontario and Quebec. Later they did buy up O&Q stock until they held 80% of it.

Along with the O&Q came land in Toronto and Montreal that is now of great value. Over the years the CPR sold off this land. Finally someone noticed that they didn't really own it, bought up some O&Q shares, and brought suit against the CPR. The case was appealed to the Supreme Court of Canada. Just before the court decision the O&Q shares were valued at $15,000 (Can.) each. A ruling for the O&Q would likely raise that by a factor of 10 or more

-- and a ruling for the CPR would drop it by a factor of 10 or more!

The court ruled for the CPR, and the stock dropped $14,100 per share in one day (and more the next day). But there was no entry in the stock market columns for this remarkable change (the stock was listed as not traded). According to the Toronto Star, "a Toronto Stock Exchange computer interpreted the sharp drop reported by stockbrokers as an error".

PacBell service "glitch"

thode@nprdc.arpa <Walt Thode>
30 June 1987 1612-PDT (Tuesday)

From the June 30 Edition of the San Diego Union:

PacBell's Service is Disrupted:
Computer glitch snarls multitude of 619 area calls

A computer program glitch disrupted telephone service in San Diego and Imperial Counties for several hours yesterday, potentially affecting all 1.1 million Pacific Bell customers in the two-county area. The breakdown came on the busiest workday of the year's busiest telephone season. A major malfunction in the computerized switching equipment at the company's main station in Hillcrest prevented many long-distance calls from going through the 619 area code, Pacific Bell spokesmen said. Affected were both local and long-distance toll calls.

Pacific bell noticed calls backing up on its monitor at around 9:30 AM. By late afternoon, technicians had traced the problem to a mysterious foul-up in the programs -- the only part of the enormous computer, installed in 1984 and working since without a hitch, that has been updated frequently, a company spokesman said. The system was shut down at 10:56 AM for 152 seconds -- a record. Then the computer had to be reloaded, trunk line by trunk line, while the search continued for the problem. By 6 PM, most of the system was back in service.

(The story goes on to describe the local impact, especially on the long-distance companies who weren't at fault.)

NASA Safety Reporting System

Jim Olsen <olsen@XN.LL.MIT.EDU>
Tue, 30 Jun 87 17:59:56 EDT

>From: Eugene Miya N. <eugene@ames-pioneer.arpa> [RISKS-5.5]
>NASA has established a voluntary, confidential safety reporting system ...

For many years, NASA has operated the Aviation Safety Reporting System (ASRS) for the FAA. It has been quite successful, producing important information about flight safety.

The ASRS has two key features to encourage participation: immunity and confidentiality. When someone reports an incident to the ASRS, he/she gains immunity from FAA disciplinary action for inadvertent errors associated with it (deliberate actions are not protected). NASA ensures confidentiality by separating the identifying information from the report during initial processing. The reporter receives a numbered receipt which can be used to prove that he/she reported the incident to ASRS. Without the receipt, the reporter cannot be identified.

The ASRS works because it offers an inducement for reporting (immunity), and provides reliable confidentiality. It probably helps that the program is operated by a trusted, independent agency.

"Information Tax" -- Risks of nonsense

Joseph I. Pallas <pallas@pescadero.stanford.edu>
Sat, 27 Jun 87 11:23:43 pdt

The notion that the proposed access charges for enhanced service providers represents some kind of "information tax" seems to be remarkably popular. Of course, it's total nonsense. The FCC is merely suggesting that Tymnet, Telenet, etc. no longer be exempt from the access charges that all other services (e.g., long distance voice) must pay for connection to the local telephone network.

The original exemption was to protect a "fledgling industry." Whether the industry can now compete on an equal basis with AT&T and MCI remains to be seen.

The computer-related risk here seems to be in how easy it is to forget that our networks are being heavily subsidized by both private and public money.

joe

"Computer woes hit air traffic" [Boston Globe, Monday, June 15, 1987]

<DAVIS%OZ.AI.MIT.EDU@XX.LCS.MIT.EDU>
Sun, 28 Jun 1987 13:33 EDT

RISKS-5.5 reprinted part of a newspaper story:

> Boston (AP) - "A computer problem that blanked the radar screens of air traffic controllers from New England to the Great Lakes for six minutes delayed flights at Logan International Airport, but posed no hazard, an official said....

This is at best vague and pointlessly inflammatory; at worst it's nonsense.

The key question is: was more than one installation affected? What exactly does "from New England to the Great Lakes" mean? If they mean more than one site, how could that have happened? Are ATC computers networked together in

such a way that a crash can propagate? (I doubt it; as I understand it they're too old to know about things like networks). If not networks, then perhaps it was a common mode power failure. At sites several hundred miles apart? I doubt it. If more than one site, then why were only the Logan flights delayed? How exactly could more than one site be affected at the same time and for the same duration? And in what conceivable sense was it "a computer problem"? A common mode software bug? One that bit all the places at the same instant?

It's considerably more likely that what they really meant was something like "One computer failed today for six minutes at Logan airport." Presumably the longer-range radar at Logan tracks some flights as far as Lake Ontario (about 500 mi). It's also possible that there are ATC centers in Montreal, Toronto, Buffalo, Detroit, New York, Cleveland, Columbus, etc. etc., (all within the same 500 mi. range) that were capable of tracking those flights, in addition to the backup system mentioned in the story. It's also interesting that there's still sufficient flexibility in the ATC system that simply slowing things down handled the problem.

The problem is that "One air traffic control system halted for six minutes today at Logan airport" and "it didn't matter at all," just isn't much of a story. Not nearly anxiety producing enough; not nearly technophobic.

Imagine the same story written with a slightly different viewpoint: "The reliability of our rather old ATC system was demonstrated today when the system at Logan airport failed completely for six minutes. Even though flites as far as 500 miles away were affected, the problem was easily handled by the existing procedures for slowing down some flights and keeping others on the ground, made possible by the routine use of backup communication systems designed for this purpose."

There are as I understand it abundant problems in getting ATC done right, ranging from reliable sw and hw to reliable organizations of people and alignment of responsibilities. It's best we attend to the real problems and try to discourage nonsense like this. Tell your local newspaper they really do have to get the facts correct.

[You can always tell a newspaper man, but you can't tell him much! PGN]

Re: Aircraft Transponders and O'Hare AIRMISS

news <mcvax!camcon!news@seismo.CSS.GOV>
25 Jun 87 13:01:43 GMT

The airmiss was allegedly due to the display equipment not showing details of an aircraft because it had a duplicate SSR transponder code...

But aircraft without an assigned code all have the same code (1234 in UK, 1200(?) in US); similarly emergency traffic all uses a small number of not-guaranteed-unique codes; so this can't be the entire explanation... (one hopes!)

Phone Company Billing Blunder

Steve Thompson <THOMPSON%BROWNVM.BITNET@wiscvm.wisc.edu>
Fri, 03 Jul 87 17:34:45 EDT

The following letter is from the syndicated column by advice-giver Ann Landers, which I saw in the 1 July 1987 (Providence, RI) *Journal*. Though it addresses real RISKs concerns, I include it more for its giggle value.

PHONE COMPANY GIVES SOMETHING FOR NOTHING

Dear Ann,

I think I can top the person who wrote complaining about the idiocy of the phone company. Talk about garbage in, garbage out!

When AT&T split with Bell, we had three phones in our house. The equipment belonged to Ma Bell and the service belonged to AT&T. After we returned all the phone equipment to Ma Bell, we received a bill for $0.00. A few weeks later, we received a check for $5 and a note thanking us. Several months later, we received another computerized bill for $0.00. We called again, got nowhere, so we sent another check for $0.00. A few weeks later we received another $5 refund with the same thank you.

This went on every three months for two years. Now we are down to once a year and have given up trying to straighten this out. We just cash the $5 and forget about it.

-- Linda K. R. in California

Stephen W. Thompson, User Services Specialist, User Services
Brown U., Box P, Providence, RI 02912 USA Smile!
THOMPSON%BROWNVM@WISCVM.WISC.EDU (401) 863-3619

Relaxed DOD Rules?

Dennis Hamilton <rlgvax!cci632!sjfc!deh0654@seismo.CSS.GOV>
Sat, 4 Jul 87 20:57:32 EDT

Here's something to chew on.

%T DOD Gives Software Developers More Leeway In Writing Code
%J Electronics
%V 60
%N 12
%P 99
%D June 11, 1987
%O Military/Aerospace Newsletter (department)
%K SDS 2167/A Top-Down Methodology Waiver
%X Military contractors no longer will be forced to use top-down methodology -- in which design and coding of computer programs use a hierarchical structure --

when developing software for the Department of Defense. The Pentagon has revised its two-year-old Defense System Software Development Standard, designated 2167, and will issue the new version, 2167/A, on June 30. The document spells out what the DOD expects from software contractors and gives them more leeway in writing code than the original standard. Although the DOD revised 2167 in response to industry dissatisfaction with the standard, some software suppliers are calling for further changes, such as provisions for rapid prototyping. Howard L. Yudkin, president of the Software Productivity Consortium, a Reston, Va., group respresenting 14 aerospace companies, is pushing for an industry position on where and how to use and not use 2167. The DOD, he says, should "recognize Standard 2167 as good for the engineering development phase for which it was intended, but not for advanced development." The Pentagon's Computer Software Management Subgroup, the joint-services committee responsible for 2167 revisions and compliance, believes that 2167 coverage of rapid prototyping is premature, according to Air Force Capt. Rick Schmidt, committee chairman.

%X That is the entirety of the announcement. Having not seen the revised standard (and not being a follower of the original, for that matter), I can't ascertain whether this is a dangerous situation or not. But it reminds me that the reputation of the Go To is being restored in the letters sections of Communications of the ACM, also.

-- Dennis E. Hamilton

Search RISKS using swish-e

Report problems with the web pages to the maintainer

Search RISKS using swish-e

THE RISKS DIGEST

Forum on Risks to the Public in Computers and Related Systems

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

Volume 5: Issue 8

Tuesday, 7 July 1987

Contents

Erasing Ford (and other) car computers

Shaun Stine <stine@ICST-SE>
Mon, 6 Jul 87 13:41:15 edt

I don't know how much this subject has been hashed/re-hashed in RISKS, but a paragraph from an article in _Mustang Monthly_ caught my eye. The gist of the article is on boosting the horsepower of the new Mustangs.

> From: "Free Horsepower for HOs!" (Mustang Monthly, July 1987)
>
> To get a more immediate horsepower boost from the elimination
> of the intake silence, disconnect the negative post on the

> battery for at least 45 seconds to erase the computer's memory.
> That way, when you crank the engine again, the computer will
> immediately begin monitoring the fuel mixture to compensate for
> the extra air flowing into the fuel injection. Be sure to
> disconnect the negative post; if you disconnect the positive
> post, the reconnection could cause a power surge that could
> possibly damage the computer.

The Mustang freaks here where I work (including myself) were interested in these tips, but as computer people, we were more intrigued by the last bit about damaging the computer and erasing the memory. A couple of questions:

1) If disconnecting the negative post will erase the computer's memory, what happens when your battery dies? Or _you_ yourself take the battery off for some reason? Does that also erase it, or does taking the positive post off within 45 seconds somehow keep you from losing the memory?

2) From that, what exactly do you lose when the memory is erased?

3) Is this mentioned by Ford manuals or any shop manuals (i.e. Chilton's)? I know dealers don't mention this - my family just bought a Sable, and I would presume that the computers are basically the same, and our salesman never mentioned it.

4) What does this do with emissions control? Some counties in Maryland have regular testing - would you still pass with the fuel being mixed differently?

Whatever information anyone could provide would be greatly appreciated. Thanks. Shaun

[A Racer's Edge becomes Erasor's Edge? Please send responses to Shaun, and he'll condense the results. PGN]

---

7 Inmates Escape; Computer Blamed!

Peter G. Neumann <Neumann@csl.sri.com>
Tue 7 Jul 87 23:13:45-PDT

On the 4th of July in Santa Fe, New Mexico, a prisoner kidnapped one guard, shot another, commandeered the control center, and released six other prisoners. All 7 went through an emergency roof door, pole-vaulted over a barbed-wire prison fence, and disappeared. The guard tower was being staffed only during daylight hours ``because of financial restrictions'' (SF Chronicle, 6 Jul 1987). A PBS item noted that the prison computer control system was down at the time, and otherwise would have prevented the escape!

Hardware failures

Don Chiasson <CHIASSON@DREA-XX.ARPA>
Mon 6 Jul 87 15:55:58-ADT

I read recently of some problems that Intel had with the 32-bit multiply instruction on their 80386 processors. I am surprised that this sort of problem does not occur more often: an obscure hardware bug which sometimes gives incorrect answers. All the emphasis is on software bugs. The assumption is that hardware will work or fail catastrophically, or that error correcting circuits will detect problems. Is this always so?

How often do microprocessors fail in minor ways? People have written about proving correctness of code: it is not possible to prove the correctness of hardware. For example, a complete test of a 32 bit multiplier would require 2**64, or 1.8E19 operations. (A year has only 3E13 microseconds.) Even without complete tests, writing diagnostic programs was extremely difficult when various margin and worst case conditions had to be considered. For example, memory diagnostic programs moved themselves around in memory; they would write bit patterns of 1's, 0's, alternating 10's and 01's, actual addresses into locations, and so on.

Hardware problems can also be bizarre. My favorite was during an experiment at sea. We were recording data, and occasionally the magnetic tape unit would hang. Putting cards on extender boards to check signals showed us that sometimes the tape was erroneously showing up busy, and sometimes the computer couldn't even find the tape. Some hours later, we found a small (1-2 mm) piece of loose wire in the back plane. As the ship rolled, the wire would sometimes short out the busy line, and sometimes short out a line which changed the physical address of the drive. We had another problem (this on land) where the card side of a backplane had been painted; tiny paint chips fell off and short/open circuited various cards. We only found it when someone took out all the cards and noticed the paint. Can't happen again? I read recently that a radar in a US fighter plane was having intermittent problems. The problem was tin whiskers which grew inside an IC, were shaken loose by vibrations and sometimes caused internal shorts. Everything repeats, only different.

Liability of Expert System Developers

Benjamin I Olasov <bloom-beacon!bolasov@husc6.harvard.edu>
5 Jul 87 22:00:58 GMT

I'm told that a hearing is now underway which would set a legal precedent for determining the extent of liability to be borne by software developers for the performance of expert systems authored by them. Does anyone have details on this?

[AIList Digest Monday, 6 Jul 1987 Volume 5 : Issue 171]
[AIList Moderator Kenneth Laws AIList-REQUEST@STRIPE.SRI.COM]

PC's and Ad-Hoc Distributed DB's

Amos Shapir <nsc!nsta!nsta.UUCP!amos@Sun.COM>
5 Jul 87 13:12:42 GMT

The last time I moved, I have noticed that certains organizations were becoming slower in accepting change of address notices. I have been receiving mail to my old address even after some mail (all computer printed) had already been sent to my new address. Some organizations had to be notified several times in writing, by phone and in person.

The latter revealed a possible explanation to this phenomenon: Many departments acquired PC's lately and kept their own personal 'phone books'; in effect they have created a distributed database, without the discipline and procedures needed to manage it. Changes to the organization's central DB did not propagate well, if at all, to these small personal DB's.

It seems that nowadays when dealing with a big organization, one has to notify them of any change in writing, so that the central DB would be updated; then by phone or in person, directly to the department one is dealing with, so that the change would *really* be done. So far this has not been a risk, only a nuisance. Horror stories, anyone?

Amos Shapir
National Semiconductor (Israel)
6 Maskit st. P.O.B. 3007, Herzlia 46104, Israel Tel. (972)52-522261
amos%nsta@nsc.com @{hplabs,pyramid,sun,decwrl} 34 48 E / 32 10 N

Risks of proposed FCC ruling

"Keith F. Lynch" <KFL@AI.AI.MIT.EDU>
Mon, 6 Jul 87 01:08:19 EDT

Perhaps it isn't correct to call it a tax - though it has never been made clear just who is to get the money. But it is hardly "nonsense" to criticize it. The same bandwidth that supports one voice link supports fifty 1200-baud data links. In practice, far more, because of packet switching - i.e., 1200-baud data is not usually sent continuously.

Charge $5 an hour for a 1200 baud link? Only if at least $250 an hour is charged for voice lines!

If this bill passes, it will no longer be profitable to sublet small slices of T1 lines. There will be no reason not use use a full 56kb voice band line even for 300 baud data.

The only ones who will benefit from this radical decrease of efficiency are those who will profit from installing unneeded new bandwidth, to be used in this inefficient manner. I say, if they can't compete in the free market, tough. Don't let them trash our freedom to communicate.

If this passes, it will keep me off the net, since my networking cost would go from $25 a month to over $2000 a month. I don't believe that anyone is subsidizing this. As far as the local phone company is concerned, it's just another local call, and it is absurd to suggest it costs them any more than any other local call. As long as competing local phone companies are not allowed, it is outrageous to allow the

one local phone company to take one's data hostage, demanding thousands of dollars for what costs them pennies, for no better reason than that they can get away with it.

I would also question how the FCC can make laws. That is the perogative of Congress, and I see nothing in the Constitution allowing them to delegate their power to unelected bureaucrats.

...Keith

RISKS in "Balance of Power"

Heikki Pesonen <LK-HPE%FINOU.BITNET@wiscvm.wisc.edu>
Tue, 07 Jul 87 16:05:15 FIN

There is a computer game about "Geopolitics in the nuclear age" called BALANCE OF POWER. It is sold at least for Commodore Amiga. I bought one and now master the beginners level -- being able to beat Soviet Union. (We Finns have tried that twice before...) I do not have time and interest to do that on the expert level, as I find many other things more interesting to do.

What does interest me is how people in the USA percieve the world view of this game. Do you think it is reasonable? There may be some risk in designing games simulating international affairs, if they are seemingly realistic. Some childish people may take them as the truth.

[Please address any resposes to Heikki Pesonen directly. Cc: RISKS if you wish. PGN]

Re: Aviation Safety Reporting System (RISKS-5.7)

<edge!doug@Sun.COM>
Tue, 7 Jul 87 10:49:59 PDT

[Although this is only marginally relevant, it raises related questions about awareness, database completeness, and ethics. PGN]

> For many years, NASA has operated the Aviation Safety Reporting System
> (ASRS) for the FAA. It has been quite successful, producing important
> information about flight safety.
>...
> The ASRS works because it offers an inducement for reporting (immunity),

I think that the past tense should be used here. I'm just going from memory, but I recall that in the late '70s the immunity provisions were dropped and ASRS quickly faded into oblivion. If it is still in operation, few pilots (including me) are aware of it.

Doug Pardee, Edge Computer Corp; ihnp4!mot!edge!doug, seismo!ism780c!edge!doug

---

A computer RISK in need of a name...

<LEICHTER-JERRY@YALE.ARPA>
29 JUN 1987 10:13:29 EST

The following appeared in the Wednesday (24-Jun) New York Times, in the Metropolitan Diary, a weekly column of "human interest" stories sent in by readers:

> A small sign was taped to a building on West 120th Street near Amsterdam Avenue, and Ellen Shaw of Scotch Plains, N.J., noticed it as she passed by. It was a discreet advertiesement for a nearby stand run by three young entrepreneurs - two boys and a girl - who were selling iced tea, cola and cookies.
>
> Ms. Shaw ordered tea and offered the youngsters a suggestion: "You may want to make a bigger sign," she said. "That one is really not to noticeable."
>
> "I know," said one of the boys, gesturing toward one of his partners, "but that's as big as his computer makes them."
>
> He paused, thought for a moment, and slapped his forehead. "Hey, I've got it!" he exclaimed. "Maybe we could DRAW a bigger sign!"
>
> The tea, incidentally, was herbal.

[As we have noted before, computers are addictive. PGN]

Search RISKS using swish-e

THE RISKS DIGEST

Forum on Risks to the Public in Computers and Related Systems

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

Volume 5: Issue 9

Thursday, 9 July 1987

Contents

BIG RED, ICEPICK, etc.

David Purdue <munnari!csadfa.oz!davidp@uunet.UU.NET>
Tue, 23 Jun 87 12:15:35 est [JUST ARRIVED, 8 JULY 87!]

> [David found some background on Donn Parker's item in RISKS-4.94.
> ``Big Red'' seems to be a Trojan horse, not a virus, but then
> the article contains a few other technical curiosities as well. PGN]

> Date: Tue 2 Jun 87 11:16:51-PDT
> From: DParker@Stripe.SRI.Com <Donn Parker>
> Subject: Australian Computer Crime [From RISKS-4.94]

>
> A sophisticated computer crime occurred in Australia recently... A
> disgruntled employee modified PC circuit boards. One called "Icepick"
> attacked ACF-2 on an IBM mainframe. The other called "Big Red" was
> used in a virus attack.

From "The Australian", Tues, 14th April 1987, page 41.

LOCAL CRIME TEAM CRACKS THE RIDDLE OF BIG RED
==========

The lethal computer virus known as Big Red has been tracked down and beaten by a team of Australian computer crime investigators, solving a riddle that has eluded foreign experts. The so-called virus has been held responsible for a string of computer disasters in several countries since it was first detected in a NASA system in the United States in 1985. It is generated by an advanced technology device planted in computer systems. At least 50 Big Red devices have been found in the US, England and Australia in banking and information-handling systems, but have never been cracked before.

Mr Stuart Gill, head of the Australian team that cracked the virus, described Big Red as a "solid state data diddling device capable of breaking encryption devices and corrupting data". Mr Gill said his team had found Big Red in the computer system of a "medium-sized Australian company that handles very sensitive information". He said the device was being used to capture and store encrypted word-processing data in the contracts division of the NSW-based company.

It was imbedded in the thick resin that had frustrated previous attempts to examine the inner workings of the system. "It is the first time anywhere in the world that somebody has been able to find one in an operating environment and find out how it works," Mr Gill said.

The investigation exposed the actual workings of the system, including its circuitry, how it is connected with computer systems, the interface with security control systems and the device's power source.

It confirmed that Big Red, frequently regarded as a part of industry mythology, operates as a parasitic operating system within a host environment. "A lot of rumours and a lot of folklore have built up around Big Red," Mr Gill said. "The device is not as sophisticated and comprehensive as it has been rumoured to be."

There is now no doubt that Big Red has the power to transfer encrypted data from legitimate files into "invisible" files, which can be accessed by users without disturbing the host's access control and encryption systems.

Mr Gill also demonstrated another suspect device, designed to function as a stand-alone system and probably used to operate an illegal gambling machine disguised as a computer game.

Both devices were found by an investigation team led by Mr Gill, one of Australia's leading experts on the unauthorised use of computer systems. His five-member investigation team took 19 hours to uncover, analyse,

anaesthetise and remove Big Red from a host computer system where it had been planted inside a terminal. The team, part of the Melbourne-based Comreco Computer Security, was called in by the company involved after management, using an audit trail, had discovered that the host system was being used after hours.

Half pages of encrypted wordprocessing data were "just disappearing off the face of the Earth". The disappearence of the pages resulted from a malfunction in the Big Red device, which normally "echoes" the appropriated data back into its legitimate file, leaving no sign of unauthorised activity. "As far as I can tell, part of the circuit was burnt out. It was there for about three months," Mr Gill said.

A circuit test procedure revealed a trace of circuit activity that was not part of the normal system's operation and the team "found the activity of Big Red as it detected that the normal system was being shut down". "I thought to myself, now that I have you, the question is where the hell are you? The system had 50 terminals," Mr Gill said.

Big Red was found in an unused terminal, where Mr Gill suspects it was planted by someone using "the old `I'm here to service the PCs' lurk". "My advice to anybody is that if you have a workstation that is going to be unused for any given length of time, pull it out," he said.

The device was identified using several criteria, including the small red LED, which gave the system its name. It lights up when the system is operational. "Its location in the communications port of the terminal, the resin casing and the red circuit board were all pointers to Big Red.

"We found it after twelve hours and it took another 7 hours to actually determine what it was doing," Mr Gill said. "I wasn't sure whether to remove Big Red from the system or bring the computer here (to Comreco's office) and surgically remove it. "Sparks flew when we pulled it out but that was all."

[The article goes on to say that this shows that Australian companies are capable of coping with high tech security, and that if American companies are thinking of setting up shop here, they will meet stiff competition.]

I can't find information that is a more technical description of Big Red, or whether they caught the person who installed the device.

DavidP

Mr. David Purdue Phone ISD: +61 62 68 8165
Dept. Computer Science Telex: ADFADM AA62030
University College ACSNET/CSNET: davidp@csadfa.oz
Aust. Defence Force Academy UUCP: ...!seismo!munnari!csadfa.oz!davidp
Canberra. ACT. 2600. ARPA: davidp%csadfa.oz@SEISMO.CSS.GOV
AUSTRALIA JANET: davidp@oz.csadfa

Air Traffic (out-of?) Control

Peter G. Neumann <Neumann@csl.sri.com>
Thu 9 Jul 87 06:51:31-PDT

The federal panel report blamed the air traffic control system itself for the Aeromexico crash, although it also blamed the entry of the smaller plane into the restricted airspace. It criticized ``limitations'' of the control system's policy of relying on pilots scanning the skies for other aircraft instead of advising planes under their control about other planes that are flying under visual flight rules. Board members also noted an apparent weakness in the radar signal, which may have made the small plane less noticeable. The safety board tried not to blame either the controller or the pilots, but said that the controller should have seen the Piper -- it was on his radar screen, although the controller has maintained it was not. (AP item in SF Chron 8 July 1987)

Last night's evening news noted that Delta Airlines has had three altercations recently -- the pilot who accidentally turned off engines and nearly crash landed in the ocean, a pilot who landed at the wrong airport in Kentucky, and a very near miss ("They could read each other's markings.").

Cause of the Mysterious Bay Area Rapid Transit Power Outage Identified

Peter G. Neumann <Neumann@csl.sri.com>
Wed 8 Jul 87 14:49:34-PDT

You may recall that BART had an unexplained power failure on 17 May 1987, unprecedented in its 15-year history. 17 switches opened for five hours, and then mysteriously closed again. On 7 July 1987 BART announced that the cause had been ascertained -- a short circuit resulted from the use of a battery charger in combination with a faulty switch. (SF Chronicle, 8 July 1987).

Sprint access code penetration

Geof Cooper <imagen!geof@decwrl.dec.com>
Tue, 7 Jul 87 11:45:27 pdt

The following is excerpted from the Peninsula Times-Tribune, Sunday, July 5, 1987. The byline is by Jack Brenan [sp?], Tribune Media Services (reproduced without permission).

> FORT LAUDERDALE, Fla. -- When Jim Wyatt received his monthly telephone bill last Tuesday morning, he got the surprise of his life -- a $14,720.96 surprise. The bill was 2-inches thick, 210 pages long, detailing 4,931 long-distance calls made on his U.S. Sprint account. Total number of minutes logged: 72,849. That's 50.6 days of non-stop talking in 30 days. ...
>
> John Frusciante, who prosecutes computer related crime for the Broward State Attorney's Office said Wyatt appeared to be the victim of one of the larger long-distance fraid cases in recent memory. ... U.S. Sprint spokesman Steve Dykes said officials had not started investigating the bill yet, but

> that Wyatt probably was victimized by a hacker who used a computer to obtain his secret access code and pass it around. ... "This is something we take very seriously. We have been beefing up our security department," Dykes said. "It's about a half-billion-dollar -- that's with a B -- problem a year for the industry." ... "Most of the time, a computer is utilized to attempt to locate valid access codes using an automatic dialer. In essence, you put it on automatic pilot and let it do its thing," Frusciante said.
>
> Wyatt ... said he made his only concern clear on the telephone [to U.S. Sprint] before he hung up. "I'm not going to pay the bill," he said.

The article is amusing, but it raises an interesting concern. The response of the U.S. Sprint people is to "beef up security." If their system was penetrated as they believe, the problem is probably better solved by improving the lock rather than looking for the thief.

The activity profile of an auto-dialer that is trying to find legal access codes is VERY different from that of a legitimate customer. It should be easy to have the computer foil such attempts (by holding the circuit open for 30 seconds and disconnecting after N attempts), to confuse such attempts (by always returning a FAILED code after the Nth attempt) or even to help apprehend the perpetrator (by flagging the line for a trace, or even tracing it automatically if this is legal).

Even if the penetration in this case was not so trivial, the article seems to indicate that the people at U.S. Sprint believe such a penetration is possible. Perhaps there should be legal recourse for customers who are inconvenienced by such inadequate security.

- Geof Cooper

Eraser's edge

Martin Harriman <MARTIN%SMDVX1%sc.intel.com@RELAY.CS.NET>
Wed, 8 Jul 87 10:10 PDT

I am more familiar with the internals of the GM system, but the GM and Ford engine control computers have enough in common that this should be true for both:

> 1) If disconnecting the negative post will erase the computer's memory,
> what happens when your battery dies? Or _you_ yourself take the
> battery off for some reason? Does that also erase it, or does taking
> the positive post off within 45 seconds somehow keep you from losing
> the memory?

If you lose battery power, the computer's volatile memory is erased. It doesn't matter whether the battery dies, explodes, is disconnected, or the computer falls off the firewall. Disconnecting the ground (negative) post has been the preferred way to remove power on cars since long before the computer era; I believe this is simply because the negative post is less cluttered.

> 2) From that, what exactly do you lose when the memory is erased?

The GM computer keeps a "crib sheet" of mixture data (indexed according to operating conditions) so that it can get close to the correct mixture without waiting for the oxygen sensor feedback, a memory of fault conditions, and some state information to help it decide whether the engine is likely to require warm-start or cold-start techniques (for instance). All this is lost when the computer loses power. If you have disconnected power, the computer will have to rebuild its crib sheet, and GM suggests that you drive for a few miles at varying speeds and throttle openings to give it the data it needs (the engine has to be warm, too, since the computer needs the feedback from the oxygen sensor).

This crib sheet is basically a set of corrections to the standard data for your engine and car; the engine computer will work adequately without it, but performance and driveability improves as the crib sheet data gets better.

Incidentally, on cars with electronic dash displays, the odometer is an electronic display of the value on a mechanical counter buried in the dash somewhere (even on cars like the GM C-bodies which have electronic speedometer/odometer systems, where the mechanical counter is driven by an electronic circuit). The GM C-bodies are "Chrysler resistant" (so to speak), since the same signal feeds the engine control computer and the odometer circuit; disconnecting the odometer (unless you get fairly fancy) also disconnects the engine computer, and this causes things not to work very well (the engine computer really likes to know how fast the car is moving, and gets upset if you're sitting at wide-open throttle and zero mph for hours at a time).

> 3) Is this mentioned by Ford manuals or any shop manuals (i.e. Chilton's)?
> I know dealers don't mention this - my family just bought a Sable, and
> I would presume that the computers are basically the same, and our
> salesman never mentioned it.

The GM shop manuals explain this quite clearly. It is possible to read most of this information out (GM cars have a little connector under the dash which includes a serial line to the computer), and some of it is quite valuable for service purposes (for instance, the crib sheet will show if the engine is running unusually lean or rich, which may indicate a leak in the intake system).

The GM computer is quite paranoid about its sensor data, too, and a large chunk of the ECM code is just checking the sensor values to see if they make sense; if the ECM decides something's strange, it records a fault code and lights the "Service Engine Soon" indicator on the dash. The fault codes can be read out through the connector, and the service manuals have flow charts for tracking down the problems indicated by the codes.

I'd be surprised if the average car salesman knew much about the engine control computer; even if he or she did, I doubt the average car buyer would be interested. I'm not surprised the salesman never mentioned it.

> 4) What does this do with emissions control? Some counties in Maryland
> have regular testing - would you still pass with the fuel being mixed

> differently?

The volatile memory (the stuff you lose when you disconnect power) is (at most) a set of minor corrections to the standard settings for your combination of engine, transmission, and options. Once the engine is warm, and you've driven a few miles and given the computer a chance to rebuild its tables, you will be (more or less) back to the state you were in before the power failure. The standard settings are all in non-volatile memory (PROMs in most cases) which won't be affected by power loss.

--Martin Harriman <martin@smdvx1.sc.intel.com>

Hardware/software interaction RISK

Alan Wexelblat <wex@MCC.COM>
Wed, 8 Jul 87 18:00:25 CDT

Friends of mine were recently stung by an unanticipated problem in the interaction of the hardware and software. They were using a random number function which was not truly random. One way to more closely approximate true randomness was to get a new seed from the system clock for each call to the generator.

When the software was being debugged, this worked fine. However, when the debugging was turned off, the random numbers suddenly started repeating (in a predictable and non-random way).

It turned out that when the software ran at full speed (without the debugging code to slow it down) it sampled the clock too quickly. Thus, the seed number was not changed and the random-number generator would produce the same number.

This bug was quite difficult to catch because it depended on the speed of series of calls to the clock-reading function. This speed was not only slightly different from execution to execution, it depended on the system load. And, of course, it changed as soon as you started to monitor it.

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

---

How to (or how not to) speed up your computer!

Willie Smith, LTN Components Eng. <w_smith%wookie.DEC@decwrl.dec.com>
08-Jul-1987 1841

From Digital Review April 6, 1987 p.75

"Victims Sought in Wall Street Fraud"

"The [S.E.C.], the U.S. Secret Service, and the Arizona attourney general's office are all investigating a reported $28.8 million computer

fraud (and a bizarre cover-up) alleged [!] to have taken place at a New York City brokerage house on June 20, 1986."

To paraphrase a bit, there is a problem during the triple witching day (hour?) when the volume of transactions skyrockets. This firm's solution to the resulting computer overload was to "speed up the operation of it's IBM computer system by turning off the applications-level software that recorded information for the audit trail for each transaction." A clever clerk set up 22 bank accounts under fictitious names for himself and selflessly volunteered for overtime that evening to help clear up the backlog. He then sold a bunch of customer's holdings and credited the money to his phony accounts, transferred the money to a numbered Swiss account, and left for 'vacation'....

The really scary part about this is that no-one knows for sure what securities he sold, who they belonged to, or how much money he ended up with! They also don't know where he is, but that's hardly surprising. :+) They wouldn't have even known that it happened except that another clerk was working on the same data and saw something change that wasn't supposed to. The firm is calling it a computer error and "hopes that customer complaints would allow it to identify and reimburse the victims."

Willie Smith w_smith@wookie.dec.com w_smith%wookie.dec.com@decwrl.dec.com
{USENET backbone}decwrl!wookie.dec.com!w_smith

Re: Aviation Safety Reporting System (RISKS-5.8)

Jim Olsen <olsen@XN.LL.MIT.EDU>
Wed, 08 Jul 87 22:26:52 EDT

I got my information on ASRS from the "Pilot's Audio Update", March 1987, Vol. 9, No. 3 (Educational Reviews, Inc., Birmingham, AL)...

NASA Safety Reporting System

<decvax!utzoo!henry@ucbvax.Berkeley.EDU>
Wed, 8 Jul 87 23:44:17 edt

It would be worth examining the [reporting systems] that do work, and they're not all in Japan: both the US and the UK have confidential aviation-safety reporting systems which get serious use. One factor which may be significant is that these systems are *not* run by the people involved in managing aviation safety! They funnel through third parties (in the US it's NASA, in the UK it's the aviation-medicine people I think) who are far enough removed from the ongoing policy wars that they can convincingly claim to be honest go-betweens. Pious proclamations of good intentions often are not enough to convince would-be reporters that their names won't get back to management.

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

Re: RISKS in "Balance of Power"

Eugene Miya <eugene@ames-nas.arpa>
Wed, 8 Jul 87 11:49:06 PDT

>From: Heikki Pesonen <LK-HPE%FINOU.BITNET@wiscvm.wisc.edu>
>Subject: RISKS in "Balance of Power"
>There is a computer game about "Geopolitics in the nuclear age" called
>BALANCE OF POWER. It is sold at least for Commodore Amiga. I bought one and
>now master the beginners level -- being able to beat Soviet Union. ...

"Beat the SU?" Chris Crawford, the author of the game, gave a talk about its development to the Palo Alto CPSR chapter before the game was marketed. His stated goal (which I might might have changed) was to have the world survive 20 years avoiding TN war. If you have beat the SU, I suggest sending a nice little letter to Chris telling him how. The fact that you are Finnish will be even more of a kick. Chris thinks, "It's only a game." He was approached by several University Poli Sci Dept. as a teaching tool.

The RISK of simulations is quite real. There exist several "games" which I hear about in the "shadows." They are played by non-computer "hard-ball" people [I was informed (at LLNL) that George Schultz was one]. I can guess it runs on an Apple II because of portability requirements. No flashy graphics. I doubt if these models are validated in anyway. Chris's game was given serious scrutiny, [the graphics were seen as a major advance, as well as the use of mice], but it apparently lacks some statistics. Note: I have not given you the name of the group which showed me this. There are other groups at the Livermore Lab (where I am allowed to visit) which do things like tactical and strategic nuclear war simulations. (I have played the most visible tactical simulation named JANUS [objective: train middle level officers use and abuse of nuclear weapons]: Blue team (me) was overrun by Red team.) There are also other National Labs, and at least 24 companies each employing close to a thousand people each who simulate matters of policy [perhaps RAND being the best known].

The US and the SU both have a propensity with technological toys. Their attraction is very powerful as adult games (lacking video). As long as the older politicians breed a healthy skepticism in the younger politicians, we are probably okay.

--eugene miya

BALANCE OF POWER

Hugh Pritchard/Systems Programming <<PRITCHAR%CUA.BITNET@wiscvm.wisc.edu<>
Wed, 8 Jul 87 10:49 EDT

> There may be some risk in
> designing games simulating international affairs, if they are seemingly
> realistic. Some childish people may take them as the truth.

About 10 years ago, here in the suburbs of Washington, DC, a video game was

introduced which simulated cars chasing pedestrians. The game was shortly removed, because people felt that the game was teaching kids that pedestrians were fair game for motorists.

On the other hand, world conflict simulations may be useful: I recall a game used in some psychology experiments. The game concerned trucks and limited roadways. The experimenters noted that the players found that cooperation between players (sharing the roadways) gained more for each player than hostile actions.

Note that 45 years ago, the Japanese war-gamed their intended attack on Midway Island. In their simulation, they lost. They proceeded with the attack, anyway. They lost the real battle, too.

Hugh Pritchard, Systems Programming, The Catholic University of America, Computer Center, Washington, DC 20064, (202) 635-5373

Search RISKS using swish-e

THE RISKS DIGEST

Forum on Risks to the Public in Computers and Related Systems

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

Volume 5: Issue 10

Thursday, 9 July 1987

Contents

Firebird computer story

Paul Kalapathy <convex!paulk@a.cs.uiuc.edu>
Thu, 9 Jul 87 09:30:23 cdt

I have a friend, Mike* (not his real name), who owns a 1983 Firebird. He does a great deal of work on cars in his spare time, but his education and job are in computer science. The work that he generally does is in microcomputers and microcontrollers. Mike was interested in improving the performance of his Firebird, and happened to have a friend John* (not his real name, either) who worked for GM and had access to the design and coding for the car computers. John was willing to provide this information

to Mike as a personal favor, and did so.

There is a PROM in the car computer that contains the basic parameters of the engine's operation, such as fuel mixture, ignition advance, temperature compensations, etc. If I remember correctly, the PROM is a type which is pin compatible with an industry standard EPROM (i.e., the EPROM can be programmed and inserted directly into the PROM position by changing only one or two power supply pins). The information in the PROM is not necessarily set for the highest engine performance, but rather to meet federal emissions control and fuel economy regulations. Therefore, changes in the parameters in the PROM could substantially improve the engine performance, to the detriment of compliance with federal regulations.

Mike proceeded to replace the PROM with an EPROM of his own programming. This resulted in a considerable improvement in the performance of his Firebird. After making this modification and adding exhaust headers to the car, it had a top speed in excess of 150mph. (After reaching 150mph on an interstate highway, Mike decided he really didn't want to know what the top speed was.) I don't recall what the top speed was before these modifications, but it was a good deal closer to 100mph than 150mph.

* "John" does not wish to be harrassed by his employer. "Mike" does not wish to be harrassed by the government for modifying polution control on his car.

COMPUTER CLUBS FOOT [DIGITAL MASSAGE?]

Anthony A. Datri <aad+@andrew.cmu.edu>
Thu, 9 Jul 87 19:10:34 edt

One risk of computers that I haven't seen addressed in this forum is the risk of having your cpu fall on you. This comes from a man who several months ago had the experience of an 11/45 falling on his foot.

anthony a datri cmu computer club

Re: 7 Inmates Escape; Computer Blamed!

Jewel <jwl@lanl.gov>
Thu, 9 Jul 87 10:17:49 MDT

The information concering the kidnapping, shooting, and release of the 6 other inmates is correct, however the rest of the information is misleading.

The guard tower was being staffed only during daylight due to financial restrictions at the time of the escape. Now it is being staffed 24 hours a day. Although the guard tower was unmanned at the time, it was not in the field of view where the prisoners scaled the fence. That area of the fence was being monitored by motion detector sensors which were attached to a computer system. Due to several false alarms, it was decided to disable

that portion of the monitoring area until the problems were solved. Also, the fence was NOT topped with the normal razor that surrounds the rest of the fences. The escape area was still under construction. The 18 foot high chain-link fence was also not covered with a fine mesh fence which made climbing the chain-link fence trivial. Normally, the fine mesh makes it near impossible to get a good hand or foot hold on the fence. It has also been mentioned that there are some design flaws in the computer surveillance system as well as the fence enclosure.

The combination of weaknesses is what made the escape possible. At present, only one inmate has been recaptured the other six are still at large, and are suspected of traveling south towards Mexico. Recent sitings have confirmed this suspicion.

James Lujan (aka Jewel)

Sprint access code penetration (catching the baddie)

Darrell Long <darrell@sdcsvax.ucsd.edu>
Thu, 9 Jul 87 15:04:32 PST

I know (personally) of one case where one of my ex-students decided that he needed free long distance. He would use his Apple-II (it was some time ago) to dial up the local number and try some number as an access code. He called the school's computer, so he knew that if he got a carrier then he had gotten through.

To make a short story even shorter, he used sequential probing to choose the access codes. The long distance company's computer (it wasn't Sprint, he'd gotten away using their's for a long time) picked up on the sequential probing. The next thing he knew there were police wandering around his house late at night. A week later he was arrested and his computer taken away (what a terrible punishment!).

The funny thing was Pac-Bell was after him to give them his "source" and find out where he had gotten the sophisticated algorithm, etc. It seems they thought he was a big time phone cracker.

Darrell Long UUCP: darrell@sdcsvax.uucp
Department of Computer Science & Engineering, UC San Diego, La Jolla CA 92093
Operating Systems submissions to: mod-os@sdcsvax.uucp

US Sprint and free long distance

Eric N Starkman <ens@ATHENA.MIT.EDU>
Thu, 9 Jul 87 12:06:47 EDT

I was reading the Wall Street Journal last week, and noticed a full page ad for the new US Sprint "FON Card." The ad included a picture of a sample card. I tried making a US Sprint call using that card number, and it worked. Further investigation revealed that ANY fourteen digit number would allow calls to be completed.

In this case, the problem was fixed by the next afternoon. But Sprint is not always so prompt. I once called them to request deactivation of a code, telling them that the security of the code had been compromised. They told me that it would take at least a week to deactivate the code.

US Sprint and the other companies claim to lose a lot of money from theft, but they are evaluating those losses based upon the retail value of the unauthorized calls.

It is only reasonable to use retail value for calls that people would have paid for otherwise. Most people I know who (would) use unauthorized long distance codes would use them only for calls which they would not have made otherwise. The real cost of the unauthorized codes, then, is simply the long distance company's marginal cost, which is negligible.

Sprint access codes (Re: RISKS DIGEST 5.9)

Edward J Cetron <cetron@cs.utah.edu>
Thu, 9 Jul 87 22:15:30 MDT

The fact that the Florida gentleman received such a large bill without warning is quite suprising. Recently, my sprint access code made its way to a similar hacker's BBoard. Within days, US Sprint called me, told me what had happened and that they were actively tracking (tracing?) the sources of the phone calls. Seems that they computer systems automagically picked up on calls being made very closely spaced in time from many different cities and that they did not fit out 'usage pattern'. When my bill came out (all 30 pages worth) there was a nice letter saying to 'just pick out the calls you KNOW are yours' which was easy since my calls all originated in Salt Lake City.

They specifically wanted the access code left live until they could try to track down the callers who were using it. They just called the other day and informed me of the new number and that of the several thousand dollars, they had recovered a great deal of it....All in all, they did a good job of keeping the customer happy and well informed, and impressed me with the capabilities of their software to extract features that indicate abuse.

-ed cetron

RE: BIG RED

<eugene@ames-nas.arpa>
09 Jul 87 10:49:20 PDT (Thu)

>... has eluded foreign experts. The so-called virus has been held responsible
>for a string of computer disasters in several countries since it was first
>detected in a NASA system in the United States in 1985.

This is news to me (unless it's a mix-up with another incident). I would

appreciate any evidence to elaborate. [Location, system type, etc.]

--eugene miya, NASA Ames Research Center, eugene@ames-aurora.ARPA
{hplabs,hao,ihnp4,decwrl,allegra,tektronix,menlo70}!ames!aurora!eugene

Risks of battery disconnections

Mahan <steve@ncsc.ARPA>
Thu, 9 Jul 87 15:24:47 CDT

In reference to the reason for disconnecting the negative terminal of a car battery: Have you ever touched (accidentally) the frame or sheet metal with a wrench while disconnecting the positive terminal?

Disconnecting the negative (ground) terminal first is a safety precaution for the mechanic to avoid inadvertantly shorting the battery to ground. After the negative terminal is disconnected the positive terminal may be brought into contact with the frame without ill effects.

steve

Steve Mahan, Naval Coastal Systems Center, (904) 234-4224.
Standard disclaimer applies.

Japanese simulation design

Sean Malloy <malloy@nprdc.arpa>
Thu, 9 Jul 87 11:53:36 PDT

> From: <PRITCHAR%CUA.BITNET@wiscvm.wisc.edu>
> Subject: BALANCE OF POWER
> Note that 45 years ago, the Japanese war-gamed their intended attack...

There were several Japanese simulations of the attack on Midway. The first simulation took into account the Japanese forces, the American forces, relative skill levels, and the like. The simulation was played, and the result of the simulation was that the Japanese lost.

This was unacceptable to the admirals, since they knew that they had a superiority in force strength, better intelligence, and the advantage of surprise, so they ordered the rules of the game to be redesigned. After a couple of iterations, playing the simulation produced a Japanese victory in line with what the admirals expected from their plans.

The attack was carried out according to the final simulation, whereupon the accuracy of the initial simulation was proved, with the Japanese losing most of their carrier force and being unable to conduct a landing on Midway.

Sean Malloy, Naval Personnel Research & Development Center, San Diego, CA,
92152-6800 (VOICE) (619)225-6434 (soon to be malloy@nprdc.mil)

Re: Hardware failures and proofs of correctness

Rob Aitken <aitken%noah.arc.cdn%ubc.csnet@RELAY.CS.NET>
9 Jul 87 5:58 -0800

In Risks 5.8 Don Chiasson notes the problem of hardware bugs, and makes the statement "it is not possible to prove the correctness of hardware". This is only partially true. A group at the University of Calgary has recently proven the correctness of a chip design and is continuing research in the area. (Anyone interested in the references can send me mail, although I add that I am not associated with this group). As for the testing of chips once the design has been verified, Mr. Chiasson is on target, as the majority of testing schemes attempt to minimize the number of defective chips released, rather than ensure that all are fault-free.

Rob Aitken Alberta Research Council, Calgary AB
UUCP: ...{utai,alberta,ubc-vision}!calgary!arcsun!rob

Hardware failures and proofs of correctness

Michael K. Smith <CMP.MKSMITH@R20.UTEXAS.EDU>
Thu 9 Jul 87 13:30:33-CDT

In response to Don Chiasson's 6 July 87 comment "it is not possible to prove the correctness of hardware". Clearly exhaustive testing is not a practical means to accomplish this. But see:

> Hunt, Warren A. Jr., "FM8501: A Verified Microprocessor", Tech. Report 47, Institute for Computing Science, University of Texas, Austin 78712, February 1986.

This is Warren's dissertation and describes the formal specification and definition of a microprocessor (similar in size and complexity to a PDP-11) and provides a proof that the formal definition satisfies the specifications. Essentially a set of mathematical operation are defined that describe the specification of the machine and these operations are shown to be equivalent to a graph of hardware gates. The mathematical operations are characterized by commonly used functions, such as addition, subtraction, and shifting. The implementation (gate graph) is characterized by Boolean functions applied to components of bit-vectors. The machine was specified and defined in the Boyer-Moore Logic and the proof was done using the Boyer-Moore Theorem Prover.

A brief, but more readily available description can be found in Bevier, Hunt, and Young, "Toward Verified Execution Environments", in Proceedings 1987 IEEE Symposium on Security and Privacy, April 1987.

This work is currently being continued at Computational Logic Inc.

- Michael K. Smith

Search RISKS using swish-e

Report problems with the web pages to the maintainer

Search RISKS using swish-e

THE RISKS DIGEST

Forum on Risks to the Public in Computers and Related Systems

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

Volume 5: Issue 11

Sunday, 12 July 1987

Contents

Old News from New Olds: Check that Backup!

<decvax!savax!nhqvax..fleischmann@ucbvax.Berkeley.EDU>
Fri, 10 Jul 87 07:07:41 edt

From the latest issue of Car and Driver page 34:

"A computer technician sent to check out a problem at Oldsmobile reports this disaster; a 70-megabyte hard disk in the company's computer system failed, completely wiping out the computer-aided design of a 1990 Olds car. Since hard disks are routinely backed up by separate magnetic-tape systems, however there wasn't much reason to panic at first. But there soon was; examination of the backup tapes revealed that they were blank. Our insider reports that Olds will have to do the design all over again."

Auto Computers [A rebootal?]

Tony Siegman <SIEGMAN@Sierra.Stanford.EDU>
Sun 12 Jul 87 10:25:28-PDT

My new Dodge Caravan has an elaborate microprocessor-controlled radio, and a large array of interior courtesy lights all linked to all the doors and hatches. If you leave any opening even slightly adjar overnight, your battery goes dead, and the radio's computer goes into a catatonic state which is NOT cured by jump-starting or recharging the battery. After battery power is restored the cassette tape will play, but the radio won't tune or respond to anything, manual or pushbutton. To restore it, you have to pull momentarily one of the two fuses supplying the radio's power. This isn't mentioned anywhere in any of the car or radio manuals; I've had to figure it out three times thus far.

Re: Liability of Expert Systems Developers

George Cross <cross%cs1.wsu.edu@RELAY.CS.NET>
Thu, 9 Jul 87 15:31:55 PDT

I don't know about any pending cases, but readers interested in this subject should check the article by Christopher J. Gill, High Technology Law Journal, Vol 1, #2, P483-520, Fall 1986 entitled "Medical Expert Systems: Grappling with Issues of Liability." An important legal issue is whether the use of a medical expert system constitutes a product or a service. If an expert system is a product, strict liability applies whereas if it a service then a negligence standard applies. Perhaps some lawyer reading Risks or AILIST could read this article and summarize it for us. It is not easy going.

- -
George R. Cross, Computer Science Department, Washington State University,
Pullman, WA 99164-1210 Phone: 509-335-6319 or 509-335-6636
...!ucbvax!ucdavis!egg-id!ui3!wsucshp!cs1!cross faccross@wsuvm1.BITNET

Re: Hardware failures

Sam Crowley <crowley%astroatc.UUCP@wisc.edu>
Fri, 10 Jul 87 11:11:58 CDT

> The assumption is that hardware will work or fail catastrophically, or that
> error correcting circuits will detect problems. Is this always so?

In the work I have done I have never made the assumption that hardware will either work or fail catastrophically. There can be a fault in hardware that will only appear when exercised. The 80386 fault only appears when certain numbers are multiplied together, otherwise the chip functions properly.

By error correcting circuits I assume you are including error detecting circuits. Error detecting methods include parity and checksums. Error correcting methods involve the use of error correcting codes (ECC) such as SEC-DED (single error correcting, double error detecting). It is possible for error detecting methods to not detect an error. With parity if an even number of bits change value there will be no error detected. With ECC it is possible for an error to be corrected wrongly or not detected at all.

A paper authored by C. Chen and M. Hsiao titled "Error-Correcting Codes for semiconductor Memory Applications: A State of the Art Review" in the March 1984 issue of IBM J. Res. Develop. magazine will explain the gory details. It should be noted that proper implementation of ECC and prompt removal of faulty parts will minimize this risk.

An error detection method to check arithmetic operations is to encode the operands in an arithmetic code. Arithmetic codes are preserved by arithmetic operations but not by boolean operations. To check a boolean operation usually involves doing the computation on two separate units and then comparing the result. A computer that did this was the STAR (self test and repair) computer designed at JPL for use on board planetary probes.

> How often do microprocessors fail in minor ways? People have written
> about proving correctness of code: it is not possible to prove the
> correctness of hardware. For example, a complete test of a 32 bit
> multiplier would require 2**64, or 1.8E19 operations.

There seems to be two issues here, design verification and testing to see if hardware is fault free. Design verification is the process of verifying that the hardware meets the specification it was designed for. I am not knowledgeable in this field. Testing to see if hardware is fault free I do know about. I have written test vectors to completely test a 74F181 which is a 4 bit ALU. It was 100% tested in around 30-40 vectors. By knowing the gate level diagram and the possible faults it was not necessary to run every combination of inputs through the chip. What was done was to setup the input vector so that a particular fault if it was present would change the output of the chip. It was written assuming that you were able to control the inputs and observe the outputs, something typically found on a chip or board tester. Tests that do not or cannot use a tester are more complicated but follow the same method of having a fault affect the output in a way that can be observed.

> Even without complete tests, writing diagnostic
> programs was extremely difficult when various margin and worst case
> conditions had to be considered.

If a diagnostic is to be effective it is going to have to take into consideration most fault cases. The tests I have worked with and written make the assumption of a single fault occurring. This simplifies the possibilities with a good probability of detecting multiple faults when they occur. Testing is simplified by the use of circuits to aid in testing the hardware. As hardware becomes more complex, testing needs to be considered when the hardware is being designed or else the test designer will have a difficult time writing tests and the tests will not be as effective as they could be.

Sam Crowley uwvax!astroatc!crowley

[Concerning SINGLE-FAULT-TOLERANT SYSTEMS, I noted recently that most of the nuclear power plants are designed to remain safe as long as only a single pipe ruptures. Two pipes are too many. Earthquakes could make things quite difficult. PGN]

Hardware/software interaction RISK <Alan Wexelblat>

"Robert Weiss" <weiss@umnstat.stat.umn.edu>
Sun, 12 Jul 87 14:27:57 CDT

>Friends of mine were recently stung by an unanticipated problem in the
>interaction of the hardware and software. They were using a random
>number function which was not truly random...

The modification described here to a pseudo random number generator (pseudo-RNG) is a really bad idea. RNG's are developed to have some basic statistical properties, such as little or no autocorrelation, a uniform distribution similar to an idealized sequence of uniform random numbers, unpredictable without a fair bit of work, non-repeating over very long sequences. Often these sequences are called pseudo-random. Whether it is possible to develop "real" random numbers is a philosophical problem.

Pseudo-RNG's have several advantages over a hypothetical sequence of "real" random numbers. For example, you can restart the generator to find the sequence of inputs to your program that caused the program to bomb. You don't need to store the entire sequence of numbers because the code to generate them is quite compact. A competent developer of a pseudo-RNG has already tested the sequences that come from the generator to make sure it indeed does pass statistical tests such as listed in Knuth's Art of Computer Programming chapter 3. When you modify the generator by changing the seed at each call, you have created a new pseudo-RNG and you don't have a clue as to the statistical properties it now has. Quite probably, you have reduced the number of possible sequences that the generator might produce - as happened to the people in Alan's story.

If you feel a need to have a higher quality pseudo-RNG than what you have available, Statistical Computing, by Kennedy and Gentle has a good discussion of various pseudo-RNG's.

Robert Weiss, Statistics Grad Student, University of Minnesota.

More on Risks in "Balance of Power"

Heikki Pesonen <LK-HPE%FINOU.BITNET@wiscvm.wisc.edu>
Sun, 12 Jul 87 21:53:53 FIN

Many thanks to all who commented on my contribution in RISKS DIGEST 5.8, "RISKS in Balance of Power". In this contribution I hope I can make it clear, why I dislike the game, although my adult children found it funny when they played it. Also in the journal Byte, May 1987, Chris Crawford's book about his game is reviewed and appreciated. In a Finnish home computer magazine "Balance of Power" received "****" (the maximum is 5 stars).

In the Instruction Manual the goal of playing is defined as "increase your geo-political prestige and weaken the geopolitical prestige of the Soviet Union."

As a beginner you proceed to the goal by

BLOWING INSURGENCY AND TERRORISM TO FLAMES.

When you master the beginner's level you can try the more difficult "intermediate level". On that a new channel of geopolitical interaction is introduced: THE SUBVERSION AND DESTABILIZATION OF FOREIGN GOVERNMENT.

You destabilize a government by sending in the CIA to encourage dissidents, fund the opposition, incite riots and create other domestic political mayhem|

After you master these affairs (besides now and then sending money and troops either to rebels or to governments) you become an expert. The Expert Level game introduces a new vehicle for governmental change, FINLANDIZATION.

Chris Crawford describes the term Finlandization by giving a short description of the history and political situation of Finland. The story is quite foolish being on the level of the tourists jokes about the polar bears they have met on the streets of Finnish cities. For example, according to Crawford:

"Finland is effectively under strong Soviet influence." and
"Finland's relations with the USA are poor."

If things are so bad, how is it possible that our recent Prime Minister and many other ministers are from the Right Party (Kokoomus). How is it possible for me to send this letter through a Finnish computer net with many IBM and Digital computers, not allowed to export to countries connected with Soviet Union? How reliable are other so called facts in Crawford's game?

In "Balance of Power" you can Finlandize a country exerting diplomatic pressure. Pressure is an attempt TO INTIMIDATE A COUNTRY WITH WORDS AND PROVOCATIVE ACTIONS, for example, holding naval maneuvers off the coast of the victim. (US Navy probably tried to Finlandize Libya when holding maneuvers on the Gulf of Syrt.)

The errors and oversimplifications of Balance of Power are not its dangerous features. What irritates me is the worldview and the type of behavior the game reinforces. Thanks to the game certainly a lot of new Oliver Norths are growing up in America. I am very glad to know, that Russians have only a few Amigas and Macs, so that their youngsters are not playing this geopolitical game.

The term "Geopolitics" is from German origin. "Geopolitik" was the strategic methodology of Nazis. Hitler was a Master level player of a game very similar to "Balance of Power".

I have written this letter in my Summer cottage not far from Russian border using my old Commodore-64 sending it through telephone lines.

Re: Sprint access code penetration

John Gilmore <hoptoad.UUCP!gnu@cgl.ucsf.edu>
Sun, 12 Jul 87 18:02:51 PDT

It is no surprise that Sprint access codes can be penetrated.
It would be no surprise to find out that AT&T calling card numbers
(basically the same thing, but mishandled) can be penetrated.

In its early days, Sprint used 5-digit access codes and assigned
them in nearby groups. This meant that knowing one or a few codes
made it possible with 15 minutes of manual trying to come up with
a bunch more. Needless to say, they were hacked to pieces.

Their response to this was the "Travelcode", a 2-digit number tacked
on to the 5-digit number when you are calling a different Sprint CO
than your usual one. They also presumably started doing more random
assignment of the numbers. Even if you knew someone's access code,
you'd have to try 50 travelcodes with it before it's likely you would
hit on the right one, and by then they could have noticed you scanning
for it.

Look at AT&T: their charge codes contain the user's phone number,
which is publicly available information. They only add 4 digits to it,
and in prior years, these digits were assigned by a trivial scheme,
which was typically discovered and published by the Yippies.

I suspect that the Telecom digest archives have a lot more information
on telephone billing security, if anyone is interested.

As with any public protestation about crime, the value is inflated.
Wholesale cocaine is always reported at inflated retail prices. Similarly,
the phone companies lose beelyuns and beelyuns of dollars at this, though
they haven't shown that it requires them to increase their call handling
capacity. What they claim to lose is the thousands of dollars that each
teenage phone hacker would have paid them making these calls legitimately.

In a recent article, someone from AT&T said "these calls have got to stop".
I challenged him, and AT&T, to stop them then. Any time is fine by me.

[This message duplicates some previous discussion, but also summarizes some
useful points and is therefore worth including in RISKS. The bottom line
is usually $, and here as usual it seems cheaper to the producer and more
acceptable to the user community to swallow the "losses". Yes, in telephone
calling it (marginally?) increases the load on the system, but in credit
cards (VISA, etc.) fraud actually results in real losses -- but they are
simply passed on to the customers through increased fees and service
charges. In both cases the burden is distributed to the users, who must
watch for unauthorized charges and then negotiate to have them undone. PGN]

Search RISKS using swish-e

THE RISKS DIGEST

Forum on Risks to the Public in Computers and Related Systems

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

Volume 5: Issue 12

Thursday, 16 July 1987

Contents

Another computer-related prison escape

Andrew Klossner <andrew%lemming.gwd.tek.com@RELAY.CS.NET>
Mon, 13 Jul 87 09:16:04 PDT

Diane Downs, a convicted murderer of some notoriety (she shot her three children, killing one, allegedly to rid herself of the responsibility for them), escaped from the medium security Oregon women's prison last Saturday. While in the recreation yard, she scaled two fences and walked away. Budget money is tight, so there was no guard assigned to watch inmates in the yard; instead they depended on an alarm system in the outer fence. The alarm did go off, but little attention was paid to it because it goes off every day,

usually because of strong winds or birds.

-=- Andrew Klossner (decvax!tektronix!tekecs!andrew) [UUCP]

[This is the problem of the system that cried "wolf!". When a system gives that many false alerts, it is time to change something to improve the false-positive discrimination. It is amazing how often this problem occurs. My neighbors next to the local high-school football field had a burglar alarm that went off whenever the home team scored a touchdown. (An intelligent thief might notice such behavior rather quickly and find safety. [2 points]) PGN]

New York Public Library computer loses thousands of book references

Peter G. Neumann <Neumann@csl.sri.com>
Thu 16 Jul 87 10:26:28-PDT

The computerized reference numbers for thousands of NYPL books were mistakenly erased when data was transferred from one computer to another. The books are still on the shelves, but have vanished from the reference system. How many are in this limbo state is unknown. A patron was quoted as having been told "by the head of research that the staff has made no attempt to retrieve them because they are afraid they might lose more if they go into the system."

Risks of being a hacker

Peter G. Neumann <Neumann@csl.sri.com>
Thu 16 Jul 87 10:32:31-PDT

Hackers 3.0 (by invitation only) is scheduled for October near Silicon Valley. The invitations indicate that the hacker community is resorting to uncharacteristic stringencies. This is from the registration form:

"I hereby waive all claims against the organizers of the Hackers Conference, their contractors, or employees, for loss of or damage to any property or injury to or death of any person at or enroute to this conference... This indemnification obligation shall include reasonable attorney's fees, investigation costs and all other reasonable costs and expenses."

Tax fraud by tax collectors

Jerry Harper <mcvax!euroies!jharper@seismo.CSS.GOV>
Mon, 13 Jul 87 14:47:22 BST

Last year in Dublin the beginnings of a major fraud were uncovered in an department of our revenue service solely concerned with rebating a Value Added Tax (VAT) paid by companies for materials they purchased. The approach adopted by the perpetrators was enviously simple due to the low

security pervading the data entry operations. Basically, the clearance system for rebates consisted of entering a company's name plus a clearance code for payment of the rebate. This information is fed to the central revenue computer for issuing cheques and what not, where a number of elementary verification procedures were invoked, e.g. was the company a database entry, etc. At this point one of the perpetrators (working with this system) could easily authorise payment blamelessly. Input from a remote terminal was overseen at the host and payment authorised. Remarkably simple. So what went wrong? The implementors of the scheme didn't manage the fictitious companies' accounts properly. When one bank manager noticed that only rebate cheques were coming into one account, he became suspicious. His suspicions were confirmed when one member of the gang demanded the withdrawal of practically the entire contents of the account. The resultant police investigation showed that the central flaw in the automatic rebating system was human. Usually before a company is granted an automatic rebate it must be in good standing with the revenue. It must prove, over a considerable period of time, that it has in fact bought the materials against which it is claiming the tax rebate. But there was no security which prevented someone administering the rebates from directly attaching a clearance code to a company. Unfortunately the system was tailor-made for criminal violation. Two more worrying aspects of the situation are that (a) due to the vast number of transactions undertaken in a year, an audit (based on sampling) would probably not have picked up any deficit; (b) if the gang had been a little less naive they could have maintained the operation for a comfortable period of time and then simply erased all record of their transactions (ok, there is the problem of backup tapes). This didn't get a lot of reportage here, but most people with any computer experience were surprised at the apparent naivete of the input/clearance system design. It was rumoured that a major review of security procedures was initiated in the aftermath of the affair.

[Note that the problem of backup can sometimes be circumvented by selectively blocking the writing of backup, or -- in some systems -- tampering with the backup copies, although that requires a little more system experience. PGN]

Re: Old News from New Olds: Check that Backup!

<utzoo!henry@ai.toronto.edu>
Tue, 14 Jul 87 13:33:07 EDT

> ...examination of the backup tapes revealed that they were blank.

For a long time now, one of our post-backup activities is to run a "table of contents" program on selected backups. The original reason was mundane: users often request retrieval of files without knowing the exact complete correct pathname and the exact date when the file vanished, so it's useful to have on-line lists that we can check. However, it also gives us a running check on the quality of our backups, which has proved particularly useful in coping with recent tape-drive problems.

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

Re: Hardware faults and complete testing

<Richard.S.D'Ippolito@sei.cmu.edu>
Monday, 13 July 1987 16:55:00 EDT

Perhaps one subtle point should be made in reference to generating a set of test vectors to 'completely' fault test a chip: I agree that it is possible to derive a test vector set when the gate-level diagram is known. But, one stumbling block that arises (and has its analog in software) is that parasitic capacitances formed due the physical layout of the IC sometimes cause the chips to have 'phantom' gates that do not appear on the schematic. We have these stray coupling problems in software -- they aren't evident from looking at our seemingly disconnected source listings, and we rarely take the time to review the operating system code with ours.

<ucbcad!ames!sdcsvax!net1.UCSD.EDU!graifer@ucbvax.Berkeley.EDU>
Mon, 13 Jul 87 23:38:00 PDT

(Dan Graifer)
To: CSL.SRI!RISKS@sdcsvax.sdcsvax.ucsd.edu
Subject: Re: Sprint Access Penetration (RISKS DIGEST 5.9)
Organization: UCSD Office of Academic Computing

I have had two interesting experiences with Sprint Access Penetration:

In December, 1986, I received a MailGram from Sprint stating that their computers had noticed a sudden, enormous increase in my travelcode usage. Having tried unsuccessfully to contact me, that had suspended the code on the assumption that it was being abused. I subsequently received a bill for about $800 in unauthorized charges. The Sprint customer service people were very helpful about issuing me a new code and advising me on how to straighten out my account. Neither they nor I were able to successfully communicate with the billing people however. It took 4 months of threatening letters in both directions to clear the matter. Apparently, GTE Sprint and U.S. Telecom were in the process of merging their billing operations, and the abuse flag on my account got lost in the shuffle.

A client of mine had a neat "deal" on long distance telephone rates. An outfit had sold them "unlimited" long distance dialing on a flat per month fee. Each day the client would call this supplier and receive a new Sprint access code to use. It wasn't until many months later that an investigator from Sprint came by asking questions. As several close friends were officers of this company, I was horrified. Does anyone out there know enough of the relevant law to comment on this? Could they be accused of receiving stolen property?

Do we have any independent estimates of how large a problem theft of long distance service is? Are the other providers having as much trouble as Sprint? (I.e., is the problem generic, or does Sprint have a uniques security hole?) My experience would seem to indicate that they are at least

trying to detect patterns of unauthorized usage.
Dan Graifer

Southern Methodist University <Leff>
Wed, 15 Jul 1987 19:16 CST

<E1AR0002%SMUVM1.BITNET@wiscvm.wisc.edu>
Subject: Phone access charges
To: RISKS%CSL.SRI.COM@RELAY.CS.NET

According to a posting on the FCC matter in the local legal bulletin board, the FCC access charge affects only public data providers such as CompuServe and Telenet. It does not affect
a) private users of modems
b) private databases such as airline reservation systems.

The theory is that long distance providers have to pay something for using the phone system. In order to compensate the local Bell Operating Company for all the calls coming in from long distance, they are given a fee. At the time this was instituted, the FCC decided to exempt such organizations as Telenet as they were relatively new services. Now that their revenue is approaching seven billion dollars a year, it was decided to a) make them pay their fair share, b) stop subsidizing them or c) tax them depending upon your point of view.

This posting also makes a statement regarding the right of Congress to delegate its law making powers. According to Kenneth Culp Davis who wrote the legal text book, Administrative Law, attacks on delegation or subdelegation "serve as a disservice to the client." Subdelegation is when Congress says that the Attorney General or some other official can make regulations and he in turn delegates it to someone such as the Immigration and Nationalization Service.

Administrative agencies have been around since the 1700's in the United States, the first handling pension issues arising out of the Revolutionary War. Mr. Davis makes compelling arguments in favor of administrative agencies, the exercise of discretion, the necessity for regulations and a balance between the "rule of law" and the "rule of men" but this is not the place to discuss that issue. I would recommend this book to anyone interested in administrative agencies.

<minow%thundr.DEC@src.DEC.COM>
Tue, 14 Jul 87 17:42:31 PDT

(Martin Minow THUNDR::MINOW ML3-5/U26 223-9922 14-Jul-1987 2028)
To: "ailist@stripe.sri.com"%decwrl.DEC@src.DEC.COM,
"risks@csl.sri.com"@src.DEC.COM
Subject: Risks in Fiction [Book Report]

From "Dirk Gently's Holistic Detective Agency," by Douglas Adams,
New York: Simon and Schuster, 1987.

"Well," he said, "it's to do with the project which first made the software incarnation of the company profitable. It was called _Reason_, and in its own way it was sensational."

"What was it?"

"Well, it was a kind of back-to-front program. It's funny how many of the best ideas are just an old idea back-to-front. You see, there have already been several programs written that help you make decisions by properly ordering and analysing all the relevant facts.... The drawback with these is that the decision which all the properly ordered and analyzed facts point to is not necessarily the one you want.

"... Gordon's great insight was to design a program which allowed you to specify in advance what decision you wished it to reach, and only then to give it all the facts. The program's task, ... was simply to construct a plausible series of logical-sounding steps to connect the premises with the conclusion." ....

"Heavens. and did the program sell very well?"

"No, we never sold a single copy.... The entire project was bought up, lock, stock, and barrel, by the Pentagon. The deal put WayForward on a very sound financial foundation. Its moral foundation, on the other hand, is not something I would want to trust my weight to. I've recently been analyzing a lot of the arguments put forward in favor of the Star Wars project, and if you know what you're looking for, the pattern of the algorithms is very clear.

"So much so, in fact, that looking at Pentagon policies over the last couple of years I think I can be fairly sure that the US Navy is using version 2.00 of the program, while the Air Force for some reason only has the beta-test version of 1.5. Odd, that."

The Other Perspective?

<baldwin@cs.rochester.edu>
Mon, 13 Jul 87 09:30:55 EDT

Last night I wandered into the TV room while my wife was watching Siskell and Ebert reviewing a movie called "Robocop" (the title should tell readers pretty exactly what the film's about). The first scene they showed involved a bunch of developers demonstrating a police robot to a group of prospective buyers - unfortunately the machine had a "glitch" that caused it to machine-gun one of the demonstrators. This scene was clearly intended to be comic, and in a grim sort of way it was. The really disturbing thing was Ebert's (I think, I don't really know which is which) later comment on this scene: "I think there's something basically funny about a machine ... blindly following instructions in

the face of logic" (quoted as nearly as possible from memory).

Now I would have said that it's been known for a long time that computers as we're building them now "blindly follow instructions" without the slightest regard for common sense or "logic", and that this is one of the fundamental sources of risks to society in their indiscriminant use. Ebert's comment got me wondering though, whether there are a lot of people out there who really do think this "feature" of machines is "basically funny", and if so how soon or effectively society as a whole is going to start demanding responsible design and use of computerized machinery.

I suppose it's not necessarily impossible to see both the humor and the serious side in a situation, and there's also the "you can't fight it, might as well laugh at it" attitude - either or both of these might (though I have no evidence) have influenced the movie makers' treatment of buggy software. From the way it was delivered and the context though, I really think Ebert meant what he said - inflexible programmed behavior is a source of humor more than of serious problems for him. I find that kind of a scary perspective.

Search RISKS using swish-e

THE RISKS DIGEST

Forum on Risks to the Public in Computers and Related Systems

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

Volume 5: Issue 13

Monday, 20 July 1987

Contents

Re: Another computer-related prison escape

Alan J Rosenthal <flaps%csri.toronto.edu@RELAY.CS.NET>
Sat, 18 Jul 87 10:58:07 EDT

Andrew Klossner:
> The alarm did go off, but little attention was paid to it because it
> goes off every day, ...

Something I've always felt strongly about in regard to this is fire alarms. There are many buildings in which fire alarms are ignored as a matter of course. I believe that in such a case having the fire alarms is worse than not having them, for two reasons. One is if you are trying to tell someone that there is a fire. You will pull the fire alarm and leave the building. No one will listen. The other is if you are trying to observe whether or not there is a fire. Someone tells you that there is, but you tend to doubt them because their information is probably from the fire alarm. At least, this could cause a delay of minutes which can be crucial in a large building in a fire.

In an apartment building I lived in recently, one night at about 4am the fire alarm went off. I blearily woke up, pulled on some clothes, and left

the building. Standing outside, I saw only two other people that felt as I did. Everyone else was still inside. (I had only been living there for two months at this time.)

Alan J Rosenthal

[If any of you wonder, "What has this to do with computers and related systems?", the answer by now should be obvious... Alarms were ignored, bypassed, misinterpreted, or otherwise mishandled in many cases such as the Stark, Three Mile Island, Chernobyl, Therac 25... PGN]

Credit card risks

David 'Witt' Wittenberg <wittenberg%ultra.DEC@decwrl.dec.com>
17-Jul-1987 1134

AT&T phone credit cards use a credit card number that consists (in most cases) of your phone number followed by four (presumably somewhat random) digits. If the last four digits are random, the probability of guessing a number (assuming you know that a particular phone number has a card associated with it) is .01%, which seems relatively safe.

The problem was that if your number was on a centrex where the main number ended in 000 all the users of that centrex had numbers that consisted of the main number followed by 4 digits (a different four digit code for each user to provide accountability), so if the centrex had 500 users with credit card numbers, a random 4 digit number appended to the centrex number had a 5% chance of working. This made the expectation value of the number of tries before finding a valid number 10!

This has been corrected, so that now the card number is an individual number followed by the 4 random digits.

--David Wittenberg

The latest in Do-It-Yourself manuals

well!bandy@lll-lcc.ARPA <Andrew Scott Beals>
Sun 19 Jul 87 16:54:46-PDT

Three ads from the August issue of Computer Shopper:

CABLE and SUBSCRIPTION TV secret manual. Build your own DESCRAMBLERS, converters. Instructions, schematics for: Sine Wave, Inband/Outband Gated Sync Pulse, SSAVI methods (for HBO, Showtime, Cinemax, UHF, etc.) Send $8.95 + $1 postage to CABLETRONICS Box 30502CS, Bethesda MD 20814.

COMPUTER UNDERGROUND. Hacking, Crashing, Pirating, and Phreaking. Who's doing it, why they're doing it, and how they're doing it. Sample programs, phone numbers, and the tools of the trade. Send $14.95 + $1 postage to CABLETRONICS Box 30502CS, Bethesda MD 20814.

HACKER'S HANDBOOK. Tells how to access remote computers, figure out passwords, access codes, operating systems, modem protocols. Plug into the electronic subculture; open up a world of new information. Send $12.95 + $1 postage to CABLETRONICS, Box 30502CS, Bethesda MD 20814.

[This item is included here to illustrate an important point: Knowledge on how to subvert system security is VERY WIDESPREAD. Sticking one's head in the sand and assuming that everything is OK is a certain way to court disaster. IMPORTANT SIDEBAR: RISKS does not endorse unsavory behavior by crackers; however, RISKS also does not endorse ostrich behavior by system purveyors. PGN]

Re: Robocop review

Eugene Miya <eugene@ames-nas.arpa>
Fri, 17 Jul 87 10:40:16 PDT

Yes, I saw that segment as well. I think the scene derived its effect from the "blame the computer" syndrome we have developed over the last couple of decades. The effect is supposed to be based on 1) "we" have this new security device, 2) to test it, would you hold this gun? [For those not seeing the scene, this biped robot security device can identify guns held at it.] Stop.

Typical person (Everyman, who was the actor of this scene, there is a name of this type of person in the Star Trek parlance) would say "No way." This is what you have test pilots and drivers for. Machines have made us think about them in less than positive ways. It's perfectly safe.

Now, for the viewer (you the reader of RISKS), do you think you would point a gun at an armed security device? Now, do ya'? Do ya' feel luck.. punk?

We (computer people) would think this device would be tested to this point. I'm certain the programmer characters in the film would have thought so too, otherwise, why would the RISKS group exist?

The problem with computer systems is that we think we should try to put common sense into them. I think this is wrong. Humans take common sense for granted. It is a form of prejudice. Common sense is not logic. The other extreme is "blind logic", which is portrayed as poor programming (actually inconsiderate "exception handling"). Our problem is that we have conflicting goals; the best written description was given by Nancy Leveson in her Computing Survey article on Safety. One purpose of science is to challenge the assumption of common sense as part of education/learning.

Remember that just over a century ago, it was `common sense' that certain members of the human population were inferior on the basis of race. Quantum mechanics arose in a different domain to change other `common sense' ideas. In the end, it is all your point of view. I do plan to see this film (as bad as it might be). S&E both gave thumbs up, but I don't trust them.

--eugene miya, NASA Ames

[1. `` `Common sense' is not very common.''

2. I have seen one scathing review and one rave
(qualified with "excessive violence").
The previews go right to the ``would you
trust this robot?'' scene... PGN]

Robocop and following instructions (RISKS-5.12)

Brian Gordon <gordon%cae780.cae.tek.com@RELAY.CS.NET>
Sun, 19 Jul 87 08:26:23 PDT

>From: baldwin@cs.rochester.edu
>"I think there's something basically funny about a machine ...
> blindly following instructions in the face of logic"

One of the scariest things I learned while teaching "Computer Appreciation" (actually titled "Computers in Society") to non-technical types in the 70's was how little college students knew about the "nature" of computers. On every final there was a question of the general type, "What are the implications of a machine that only does EXACTLY as it is told". The majority of the answers were always about how bad it WOULD be if there WERE such devices -- and remember, this was after they were told the question was coming! It almost makes you want to take up plumbing.

FROM: Brian G. Gordon, CAE Systems Division of Tektronix, Inc.
UUCP: tektronix!cae780!gordon [or gordon@cae780.CAE.TEK.COM]

Re: Robocop review

<baldwin@cs.rochester.edu>
Mon, 20 Jul 87 11:35:48 EDT

Right-on-target discussion (by Eugene Miya) of safety and risks in this hypothetical situation, and the contrasts between what people intuitively expect from "intelligent" machines and what they actually get. (The term "intelligent machine" is a lasting disservice done to our discipline by the press of the 1940's and '50's.) The point I want to make is that there seems to be a large segment of society out there that doesn't think this is a risk at all - it's just funny. That's the same society that somehow has to make collective decisions about computer systems in nuclear power plants, weapons, planes, and all the other things we've been discussing for who-knows-how-long here.

Search RISKS using swish-e

THE RISKS DIGEST

Forum on Risks to the Public in Computers and Related Systems

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

Volume 5: Issue 14

Wednesday, 22 July 1987

Contents

FAA absolves Delta in 2 close calls, ATC problems blamed in one

Peter G. Neumann <Neumann@csl.sri.com>
Wed 22 Jul 87 11:17:40-PDT

There were two near-misses last weekend -- two Delta jets over Virginia both bound for Dallas-Fort Worth, and a Delta jet and a single-engine Cessna approaching Sacramento. In both cases the FAA reported that the Delta jets were "just following instructions" from the air traffic controllers. In the first case, the Atlanta ATC center in Atlanta was having computer problems and the FAA placed the blame there -- on the system or on the controllers.

In the Sacramento case, it appears the private pilot was at fault. (Delta has been having an incredibly Murphian run of bad luck lately, with about ten different incidents in the past two weeks.) [Source: SF Chronicle, 22 July 1987]

Incidentally, the July/August 1987 issue of the Common Cause Magazine has an article by Jonathan King entitled "Blind Spots", "another reason to fear flying: faulty air traffic equipment and not enough manpower to keep it working." It is a reasonably sensible analysis of past troubles.

Origin of term "intelligent machine" - press probably not responsible

Jon Jacky <jon@june.cs.washington.edu>
Wed, 22 Jul 87 09:28:40 PDT

> baldwin@cs.rochester.edu writes:
> The term "intelligent machine" is a lasting disservice to our discipline
> by the press of the 1940's and 1950's..."

I'm not sure what the original source of this phrase was, but the term "artificial intelligence" was originated in the 1950's by John McCarthy, generally regarded as one of the most important computer scientists (he invented LISP, among other things). The story goes that he created the term in a grant application in order to kindle funders' interest in topics like symbolic logic with otherwise seemed rather esoteric and impractical.

I am getting tired of people blaming "the press" for "sensationalizing" items that were in fact originally sensationalized by the technical community itself. In fact the most mind-boggling and incredible claims about computing often originate from some scientists, and are if anything underreported by the press. For example some quite well-regarded computer scientists are said to believe it will be feasible to load a runnable copy of a human intelligence into a computer in the reasonably near future, so we won't have to die anymore. What has the NATIONAL ENQUIRER got that can beat that? A particular galling example to me is DARPA people complaining about the "misconception" that Strategic Computing is promoting "killer robots" when in fact their reports picture autonomous flying vehicles dropping bombs on things.

- Jon Jacky

---

robocop

Lou Steinberg <lou@aramis.rutgers.edu>
Wed, 22 Jul 87 11:25:17 EDT

I think there may be some overreaction here to the comments on a machine blindly following instructions as a form of humor. In fact, *people* doing this kind of thing, especially taking things literally that were meant figuratively, is a classic form of humor. Gracie Allen was a master at this.

[Yes, even for those who remember Gracie, let's go slow here on people

blindly following instructions, unless there is a RISKS connection. PGN]

Nuclear power plants

Alex Bangs <bangs%husc8@harvard.harvard.edu>
Tue, 21 Jul 87 15:54:25 edt

I am very interested in nuclear power plant control. I was wondering if there are any books/articles that people might recommend on the subject. It is my opinion (and this ought to get some people going) that if they could actually build one of the plants without construction corruption, we might be able to have a nuclear industry. It is also my belief that some intelligent (see: Robocop) control systems ought to be able to keep a plant running safely, given mechanical backup.

Alex Bangs, Harvard Robotics Lab, bangs@metatron.harvard.edu

Nuclear power plants

<Nancy Leveson <nancy%murphy.UCI.EDU@ROME.UCI.EDU> [at PGN's request]>
Tue, 21 Jul 87 21:20:44 -0700

Alex Bangs brings up two points with respect to nuclear power plant control:

> >It is my opinion ... that if they could actually build one of the plants
> >without construction corruption, we might be able to have a nuclear industry

Although there have been construction foulups, I doubt that they can all (or even most) be tied to corruption as opposed to simple mistakes. The reasons for the nuclear power industry problems go way beyond construction difficulties and include economics, poor management, limitations in our basic engineering capabilities, the impossibility of building any complex systems that need to guarantee an extremely low failure probability, etc. For an excellent discussion of these problems with respect to the nuclear power industry and other complex systems, I highly recommend a book by Charles Perrow called: "Normal Accidents: Living with High-Risk Technology" and published by Basic Books in 1984.

> >It is also my belief that some intelligent (see: Robocop) control systems
> ought to be able to keep a plant running safely, given mechanical backup.

Computers are currently used in nuclear power plant control, but I assume Alex is suggesting that computers be given complete responsibility for safety. I have not seen Robocop, but from the descriptions in Risks of the robot following orders and killing someone inappropriately, I would hate to think that this is the way we would want to build a nuclear power plant. But more seriously, it is important not to confuse Hollywood with reality. AI software has not proven to be any more reliable than any other software. Programming is programming whether the application is supposedly intelligent or not. I will try to avoid controversy by refraining from commenting on the capabilities of supposedly "intelligent" systems, but

it seems reasonable that if we were able to guarantee perfect software that way, all software would immediately be written using AI techniques (or more cynically, labelled as "intelligent") and we could all stop writing into and reading the Risks bulletin board.

Considering everything, it does not appear to be reasonable or responsible to depend on software to guarantee safety in any system where the consequences of failure are as extreme as in nuclear power plants. Note that this does not mean that computers cannot be used in these systems -- they currently are.

It only means that we cannot expect computers to eliminate the danger of nuclear power plants or any other complex, potentially unsafe system. The systems with computers are likely to be as dangerous as without them, and because of the well-known difficulty of building highly reliable software, they may be LESS safe with computers. Whether we can in the future learn how to use computers to control safety-critical systems with the same or less danger than without them is still unknown, but there are no simple answers.

Nancy Leveson (nancy@ics.uci.edu)
Information and Computer Science, University of California, Irvine

Reminder about alarms

<eugene@ames-nas.arpa>
21 Jul 87 09:58:09 PDT (Tue)

> [If any of you wonder, "What has all this to do with computers and related systems?", the answer by now should be obvious... Alarms were ignored, bypassed, misinterpreted, or otherwise mishandled in many cases such as the Stark, Three Mile Island, Chernobyl, Therac 25... PGN]

Addendum, especially in the case of Chernobyl and Brian's Computers and Society comment later in the same issue. We, computer people, are frequently accused of a binary mentality. This is a good case where we have a minimum of three states: true alarm, false alarm, and testing/practice. The last case is important because it allows consideration of further contingencies, but it has the further danger of true alarm during testing/practice as well as known false alarm. The complexity can get worse, so I won't go into it. The question is how to provide for testing?

I hope that the situation will not get worse before it gets better. Like "Robocop," I have to remain skeptical. We (computists) are the guardians for the general public at this time.

--eugene miya

FCC computer fees

Alex Bangs <bangs%husc8@harvard.harvard.edu>
Tue, 21 Jul 87 15:40:20 edt

I can see the point that the FCC should be able to tax an industry that is no

longer completely weak, but there is still a problem. First, the people who are probably going to get taxed are the users, not the company. Perhaps if they drop their prices or lose users, their profits will drop. Otherwise, the government will just be making more money while Telnet continues to make big profits. The other problem I see is that this system really hurts the small-time home user of these services. I really cannot afford to use CompuServe at more than $6 per hour for fun. In a way, this tax is still risking damage to the home compute culture.

Alex L. Bangs, Harvard Robotics Lab, bangs@metatron.harvard.edu

Risks of exporting technology

Clint Wong <cgwong%orchid.waterloo.edu@RELAY.CS.NET>
Wed, 22 Jul 87 10:40:45 EDT

July '87 IEEE Spectrum - Newslog

Norway will tighten export controls on technology. The Defense Minister announced this decision following disclosures that the state owned Kongsberg Vapenfabrik sold metalworking machines and related software to the Soviet Union. The equipment was sold in partnership with Toshiba Machine Co. of Japan and enabled the Soviets to build quieter submarines using advanced propellor blades.

> [Some of you have seen Monday's full-page ad from Toshiba apologizing for this event, and promising never to do it again. This case reminds us of some critical risks in technology outflux and some other critical risks when there is not relatively equal distribution of technology... Evidently this is a case in which the President's offer to share (e.g., the Star Wars technology!) is not applicable -- it seems to have had a very profound effect. (There is the old joke about certain computer systems and programming languages that should be given to our adversaries in order to set THEM back many years. On the other hand, nuclear weapons capabilities are a case in which maintaining parity among the main parties does not help stave off developments in other nations.) (End of ramble.) PGN]

Electronic Cash Registers

William Daul / McDonnell-Douglas / APD-ASD <WBD.MDC@OFFICE-1.ARPA>
21 Jul 87 18:29 PDT

I forgot to send this comment to RISKS a few months ago. I purchased some goods at a electronic register...the type that tells you how much change the customer is to receive. When I started looking at the facts (cost of item, amount tendered and change), I realized that register had the wrong amount displayed.

Can someone tell me how common a problem is this? Have others run into it? It makes me a bit cautious now. Any comments or pointer to further information

would be appreciated.

[Responses to Bill, please. PGN]

Brief book review of the Hacker's Handbook

John Gilmore <hoptoad.UUCP!gnu@cgl.ucsf.edu>
Wed, 22 Jul 87 18:50:28 PDT

The mention of the Hacker's Handbook reminded me of this book.

> The Hacker's Handbook, by Hugo Cornwall. 1986 edition. Published by E. Arthur Brown Company, 3404 Pawnee Drive, Alexandria, Minnesota, USA 56308; phone +1 612 762 8847. ISBN 0-912579-06-4.

I found it last year and really liked it. The book is written from a European perspective (it was originally published in England). It starts from basics of computers, modems, and security, mentioning a lot of things that RISKS readers already know very well. But it includes numerous examples of hacking European data services, e.g. Prestel, British Telephone, various X.25 networks, the British MI5 intelligence service, as well as radio data hacking . There was sufficient "new" information to keep me avidly reading all the way through. The author's writing is chatty and informative, very easy to read. I recommend this book for the Risks Library.

Re: Credit card risks (RISKS-5.13) [plus a robopoem]

Amos Shapir <nsc!nsta!nsta.UUCP!amos@Sun.COM>
22 Jul 87 14:57:41 GMT

wittenberg%ultra.DEC@decwrl.dec.com (David 'Witt' Wittenberg) writes:
>AT&T phone credit cards use a credit card number that consists (in most cases)
>of your phone number followed by four (presumably somewhat random) digits.

When I realized that, and that the only purpose of the card was to remember the number, I memorized the last 4 digits and destroyed the card. The possibility that someone who knows my name (e.g. in the office) will look over my shoulder while I was using it was just too great.

Even now when the cards are nagnetic there's not much point in keeping them, as there are as many systems that accept regular credit cards wherever the AT&T machines are.

Subject: Re: Robocop and following instructions (RISKS-5.12)
Brian Gordon <gordon%cae780.cae.tek.com@RELAY.CS.NET> writes:
> >From: baldwin@cs.rochester.edu
> >"I think there's something basically funny about a machine ...
> > blindly following instructions in the face of logic"

I really hate this damn machine,
I wish that they would sell it;
It doesn't do quite what I want -
Only what I tell it!

-- Funny, but also a Major Truth.

Amos Shapir, National Semiconductor (Israel)
6 Maskit st. P.O.B. 3007, Herzlia 46104, Israel Tel. (972)52-522261
amos%nsta@nsc.com @{hplabs,pyramid,sun,decwrl} 34 48 E / 32 10 N

Search RISKS using swish-e

THE RISKS DIGEST

Forum on Risks to the Public in Computers and Related Systems

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

Volume 5: Issue 15

Thursday, 23 July 1987

Contents

Access by 'hackers' to computer not criminal

Robert Stroud <robert%kelpie.newcastle.ac.uk@Cs.Ucl.AC.UK>
Thu, 23 Jul 87 13:02:45 BST

Regular RISKS readers will remember the case of Stephen Gold and Robert Schifreen who broke into the British Telecom Prestel network and were successfully prosecuted under the UK Forgery and Counterfeiting Act of 1981

last year. I believe they were responsible for breaking into Prince Philip's [demonstration] mailbox on the system. [See RISKS-2.44.] Anyway, this was a test case and it went to the Court of Appeal. Last week the judges decided to allow the appeal. As a result it would seem that under English Law

> The dishonest obtaining of access to a computer data bank by electronic means is not a criminal offence.

I am not a lawyer so I am not sure I can explain the legal arguments behind this decision accurately! I am not even sure from the legalese whether they got off on a technicality or not! However, it would appear that existing law cannot be applied to computer hackers.

What follows is based on the account of the decision given in the Law Report section of The Independent dated Wednesday 22nd July 1987 by Simon Cassell, Barrister. (c) Copyright Newspaper Publishing PLC 1987

The legal reference is Regina v Gold and Schifreen, Court of Appeal (Criminal Division), 17th July 1987.

Under the terms of the Act, Gold and Schifreen were charged with "making a false instrument on, or in, which information was recorded or stored by electronic means, with the intention of using it to induce the Prestel computer to accept it as genuine, and by reason of so accepting it to do an act to the prejudice of British Telecom plc".

At the root of the case was the question of what this false instrument was. In the original ruling, the judge stated that "... the defendant here made a series of electrical impulses which arrive at, affect and operate on what is called a user segment". The two candidates for the false instrument were therefore the electronic impulses and the user segment.

The defence argued that the electronic impulses could not be a device since they simply carried information, being no more than a translation of the customer identification number (CIN) and password. The court agreed.

The prosecution argued that the user segment was modified by the CIN and password which it recorded momentarily in order to check they were genuine. This was the false instrument manufactured by the appellants and the fact that it had only existed for a brief moment of time was immaterial.

The court disagreed with this on three grounds.

(1) A forgery is a document containing messages of two kinds: a message about the document itself (e.g. that it is a cheque), and a message in the words of the document that it was to be accepted and acted upon (e.g. that a banker was to pay a certain sum of money). The user segment did not contain both these types of message at the moment when it was supposed to be a forgery.

(2) The Act did not seek to deal with information that was held for a moment while automatic checking took place and was then expunged.

(3) The prosecution had to prove that the appellants had intended someone to accept the false instrument they had made as genuine. But the machine (i.e. the user segment) which it was intended should be induced to accept the false instrument seemed to be the very thing which was said to be the false instrument (i.e. the user segment) which was inducing the belief. If this was a correct analysis, it reduced the prosecution case to an absurdity.

The judges concluded that the language of the Act was not intended to apply to the situation which was shown to exist in this case, and "the procrustean attempt" to force the facts to fit the Act "produced grave difficulties for judge and jury which the court would not wish to see repeated." What the two individuals had done amounted to a trick. If it was thought desirable to make this a criminal offence, "it was a matter for the legislature rather than the courts."

<End of Legal summary>

It is not clear to me as a non-lawyer whether a more carefully drafted charge which specified the false instrument as being the micro computer and modem which Gold and Schifreen presumably used to gain access would have succeeded. However, it will be interesting to see in the light of this decision whether some specific legislation is drafted to make hacking a criminal offence. The whole area would seem to be a legal minefield at present!

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

On expecting the unexpected in nuclear power plants

David Chase <rbbb@rice.edu>
Wed, 22 Jul 87 23:54:42 CDT

On nuclear power plants, and making them work--unforeseen problems arise. For example, at the South Texas Nuclear Project, one unexpected problem was ... clams growing in the cooling water pipes. You'd like to filter them out, but their larvae are very very small. You'd like to poison them, but the water is kept in great big ponds that could percolate slowly into the clay. What to do?

As if that weren't enough to test your foresight, I believe that these clams are exotics (i.e, illegal alien species). In spite of the bad press that technology has received over the years, purely natural problems can be (I think) just as bad. Consider, for example, fire ants, killer bees, hydrilla, water hyacinths, and citrus canker. On the other hand, manatees (which eat hydrilla, though not as quickly as it grows) like the cooling water outlets from the Crystal River Power Plant. Florida Power has this great bumper sticker, "I Brake for Manatees". It was a bit of a coup for the power company. [There was more on alligators in the Indian Point (River?) plant cooling water canals...]

David

[Let's hear it for Hugh Manatee. P.]

Risks of Nuclear Power

Mark S. Day <MDAY@XX.LCS.MIT.EDU>
Thu 23 Jul 87 11:17:03-EDT

It is worth noting, too, that nuclear power is not only risky when things "go wrong" (e.g. bungled construction, operator/control errors) but also when things "go right". A normally-operating fission reactor produces large amounts of wastes that are dangerous for longer than the lifetime of a typical plant, and smaller quantities of wastes that will be dangerous for millenia.

We would all do well to remember that our solutions to current problems should not create worse problems in the future.

Chernobyl predecessors?

<mnetor!utzoo!henry@uunet.UU.NET>
Thu, 23 Jul 87 15:32:23 EDT

In a recent issue of Science there was a long article by an American scientist who had visited Chernobyl and talked to all the major people involved in the response to the accident. It makes interesting reading. He measured radiation in the area; nothing very serious any more, in the sections he visited. Several aspects of the cleanup were being delayed by cold weather, e.g. replacement of contaminated tar on building roofs. There is an implicit comment that attitudes towards radiation have changed: outside the immediate vicinity, the fallout from Chernobyl was similar in magnitude to that of a very large atmospheric nuclear test -- an event that was not uncommon in the 50s, albeit usually in more isolated areas. In general he was impressed by the speed and competence of the Soviet response to the mess. The medical handling of the situation, in particular, was so rapid and skilled that it strongly suggests they've had practice at this. He also notes that the other reactors at the plant were back in operation within a year -- a considerable contrast to Three Mile Island #1, an undamaged and perfectly functional reactor that sat idle for the better part of a decade.

His overall assessment of the cause of the disaster agrees with the common consensus: a somewhat hazardous reactor design combined with truly major ignorance and carelessness by the operators. He notes that just making more rules for the rank-and-file operators would not have solved the problem, because it was one of the senior engineers who was responsible for most of the violations of normal operating rules. As an immediate precaution, the operators are now told that the plant management is *not* authorized to override the basic safety rules. Much more attention is now being paid to operations issues in general, and some modest modifications to the reactors have also been made. The real solution is to use a safer reactor design, but the worker's paradise is no more willing to scrap a dozen power plants overnight than the dirty capitalists would be.

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

Who's responsible - ATC or pilots

Andy Freeman <ANDY@Sushi.Stanford.EDU>
Wed 22 Jul 87 23:49:22-PDT

In the July 22 issue of the SF Chronicle, page 20, Layne Ridley wrote an article about flying fears. (This is the same issue that reported that two Delta incidents are being blamed on the ATC, not the pilots.) Part of the response to "The pilot is drunk or incompetent." is:

> The captain of an airliner is held legally responsible for every aspect of the flight. No matter if he or she was acting in good faith on instructions from the airline, an air-traffic controller or anybody else, if an plane under a captain's control is involved in any infraction or incident, the captain will be suspended, guilty until proven innocent.

What are the pilot's responsibilities and liabilities? What about the controller's?

-andy

"Intelligent" control

Alex Bangs <bangs%husc8@harvard.harvard.edu>
Thu, 23 Jul 87 12:04:59 edt

>From Nancy Leveson <nancy%murphy.UCI.EDU@ROME.UCI.EDU>
>The reasons for the nuclear power industry problems go way beyond
>construction difficulties...

Oh yes, I realize that. I just hate it when people are dishonest when it comes to such critical safety issues; it reads too much like a horror movie, but it's for real. As for economics and engineering, I realize that those are problems. Sorry for presenting such a simplified view without explanation.

>I have not seen Robocop, but from the descriptions in Risks of the robot
>following orders and killing someone inappropriately, I would hate to think
>that this is the way we would want to build a nuclear power plant...

Again, please allow me to clarify. I am talking about systems that would only have the intelligence to help watrch for operator mistakes (like noting that a valve has been open for longer than it normally should), and helping to consolidate information in case of a major alert--summarizing the critical information and making suggestions for courses of action. Basically, I envision a system that is similar to the direction being taken in cockpit avionics. With such a system, however, there is a risk that is the bane of all pilots--boredom. For a wonderful set of information on aviation risks, see the November 1986 issue of IEEE Spectrum. I don't suggest reading it on a plane :-)

I have no intention of ever letting a computer run a nuclear power plant, or the US ICBM system (see WarGames). We are not at that stage, and I am not sure that we ever want to be. Computers can be useful in presenting information in a useful fashion. Making decisions is another matter altogether.

Alex Bangs, Harvard Robotics Lab, bangs@metatron.harvard.edu

Just a quick addition. John Page, from our lab, suggested that the computer ought to call up the NRC on operator overrides and request that they come take a look, i.e. the computer plays the rat :-) Alex

---

Taxes and who pays them

William L. Rupp <nosc!rupp%cod.nosc.mil@sdcsvax.ucsd.edu>
23 Jul 87 15:29:41 GMT

In a comment on the propsed FCC data transmission fee, Alex Bangs states that in this case the "users, not the compay" will pay the tax. I would just like to comment that in *all* cases it is the users, or customers, who pay the tax. I.e., the company gets all its money from what it charges the buyers, and must therefore pass along increases in taxes.

My comments reflect neither agreement with nor oppositon to the FCC proposal. I just wanted to clarify that one point.

My Usenet comments are strictly my own opinions.

Computer Know Thine Enemy (Reference); Reactor control-room design

<eugene@ames-nas.arpa>
23 Jul 87 10:22:49 PDT (Thu)

>... "misconception" that Strategic Computing is promoting "killer robots" ...
> - Jon Jacky

An interesting reference just appeared (I don't normally read this publication):

%A Andrew Borden
%Z TRW
%T Computer Know Thine Enemy
%J AI Expert
%D July 1987
%P 48-54
%K Bayesian analysis, aerial combat, battle management,
%X No comment.

Re: Reactor control room design

This is regarded in several sectors as an increasingly sensitive subject, and I am of the growing opinion that it not appropriate to discuss

this subject in an open forum. Readers should also note that several of the FORMER readers have included `experts' in this field.

--eugene miya, NASA Ames Research Center

Medical computer risks?

Prentiss Riddle <ut-sally!im4u!woton!riddle@seismo.CSS.GOV>
22 Jul 87 17:02:18 GMT

This is a request for information: can any of the readers of this list provide examples of problems caused by computer errors in the medical field?

[Presumably the requestor has been following the Therac-25... PGN]

I would especially be interested in any relating to loss or damage of electronically stored medical records and medical orders. My institution is in the process of purchasing a Patient Data Management System (PDMS) which is supposed to eliminate the use of paper recordkeeping in an intensive care unit. It will hopefully provide a significant improvement in the speed, detail and reliability of patient charting, but there is also clearly an element of risk involved. Some horror stories might help us open our eyes a bit and avoid repeating anyone else's errors.

--- Prentiss Riddle
--- Opinions expressed are not necessarily those of Shriners Burns Institute.
--- riddle@woton.UUCP {ihnp4,harvard,seismo}!ut-sally!im4u!woton!riddle

---

Electronic cash registers

Thu, 23 Jul 87 10:42:44 EDT

I response to your note in RISKS:

I recently stopped at a nearby supermarket to purchase milk. I chose the cheapest brand (not an easy task, since the labels on the shelves were very poorly maintained and the packages are not marked at all).

When the clerk scanned the cartons the register rang up a price considerably higher than what was on the shelf (though not enough higher to be noticable in the middle of a large bill). Since I was only buying one item, I *did* notice the difference and objected. The clerk went off to check with somebody, then gave me the lower price.

What was truly amazing was the reaction at the customer service counter when I stopped to complain. I was informed that, yes, the prices in the store's computer do not necessarily match the prices marked on the shelves, and the customer who isn't careful may get cheated. I received the impression that mine was a relatively common experience and that the store did not consider it a problem.

I sent a very formal, very strongly-worded letter to the store manager, but received no reply.

<Michael Wagner +49 228 303 245>
Thu, 23 Jul 87 15:58 CET

<WAGNER%DBNGMD21.BITNET@wiscvm.wisc.edu>
Subject: Re: Credit card risks (Amos Shapir, RISKS 5.14)

There must be something very different about the way Bell Canada
calling cards work, or else I missed the point somewhere.

> >AT&T phone credit cards use a credit card number that consists
> >(in most cases) of your phone number followed by four
> >(presumably somewhat random) digits.

I suspect this is only true in some cases. It's certainly not true for me.
The first 10 digits of my credit card number are some random telephone
number in some exchange I've never heard of. It's certainly not my
telephone number. I don't even have a Canadian telephone number, currently.
[Actually this is true of several of the nonAT&T carriers.]

> When I realized that, and that the only purpose of the card was
> to remember the number, I memorized the last 4 digits and
> destroyed the card.

But that's not the only use of the card. My card, at least, has 2 numbers
(and a mag stripe that we'll come to later). The second number is an
international calling card number, good (in theory) outside North America
(in practice, no one in Western Europe seems to honour it yet, but I keep
hoping).

> The possibility that someone who knows my name will look over
> my shoulder while I was using it was just too great.

I can't imagine what difference knowing your name makes. They
never ask me what my name is. In any case, 'they' can look at
your fingers pushing the keys on the telephone just as easily as
at the card. Actually, the mag stripe is safer in this respect;
you never have to hold it still in anyone's line of vision.

> Even now when the cards are magnetic there's not much point in
> keeping them, as there are as many systems that accept regular
> credit cards wherever the AT&T machines are.

This doesn't seem to match my experience.
(a) I've been to many places where the credit card machines only
take telephone cards.
(b) some credit cards cost more for the same phone call. At the
least, there is the service charge for the use of the card.
(c) the audit trail isn't as good. When I have used VISA to make
a phone call, I get back, on my VISA account, an undecodable
string of digits. When I use my calling card, I get a line

item on the standard telephone bill in a standard,
comprehensible format.

All in all, I'd say there is a lot of point in keeping the card
and using the mag stripe.

Re: "The Other Perspective?"

<baldwin@cs.rochester.edu>
Thu, 23 Jul 87 09:15:04 EDT

>From: Heikki Pesonen <LK-HPE%FINOU.BITNET@wiscvm.wisc.edu>

>According to my opinion, the risk that computers blindly follow
>instructions is not so high than the risk that people
>blindly follow orders. So they have always done, but the risk
>is greater nowadays, when we have the so called advanced technology
>in our hands. ....

True - people blindly following orders are probably worse
than computers doing it. The intent behind my original posting though
(which seems to have been widely missed) is that an even bigger
potential risk is that some large fraction of non-technical society
(a) doesn't realize that there ARE risks in the use of computer
technology (no surprise there really), and (b) when shown risks,
these people do not say "hey, that's a problem", they say "hey, that's
a good joke". At least in places (if any :-) where democratic government
works according to theory, those same people help make decisions about
some rather critical, risky uses of computers ("Shall we spend
X billion dollars on computerized anti-missile defenses?", "It must
be OK to build the new nuclear power plant, the computer simulations
say it's safe", etc.) Depending on how widely people really mistake
serious risks for funny glitches, we have a situation in which the
people deploying new technology (at least in a broad policy sense)
may neither know what they are doing, nor realize that there are
important things that they don't know. This, to my mind, is a much
more serious risk (or meta-risk) than the failure of particular languages
to check subscript limits or whatever.

I guess what I hope to do was get some discussion/feedback
on this kind of meta-risk going (other instances? does it really exist or
am I just a pessimist? what can/should be done about it? etc.) Apologies
if earlier postings didn't make this clear.

Search RISKS using swish-e

THE RISKS DIGEST

Forum on Risks to the Public in Computers and Related Systems

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

Volume 5: Issue 16

Saturday, 25 July 1987

Contents

$23 million computer banking snafu

<Hoffman.es@Xerox.COM>
24 Jul 87 08:11:36 PDT (Friday)

Edited and excerpted from the Los Angeles Times, Friday, July 24:

$23-MILLION COMPUTER SNAFU ADDS TO BofA'S TROUBLES

Bank of America quietly acknowledged a $23-million computer snafu that is alienating key customers and will likely take months to fix. The one-sentence disclosure in the company's second-quarter financial report said, "the corporation established a reserve for estimated costs, arising from problems in Bank of America's conversion to a new trust accounting and reporting system, which reduced net income by $23 million."

The problems arose when a new system, MasterNet, was brought on line in March before being fully debugged to replace an aging system. "They committed two cardinal sins," a trust dept. official said. "They took down the old system before the new system was up and running. And they were the first big bank to install the system. A key rule in computer software is: Never go first."

As a result, sources say, the system has crashed for days at a time, the bank is months behind in providing customers with their monthly statements and there have been potentially costly delays in trading securities. Sources called it a major embarrassment. "Heads are going to roll."

The institutional trust services department administers more than $38 billion in pension fund and other assets for more than 800 corporations, unions, and government agencies.

MasterNet was designed by Premier Systems Inc., a Wayne, Pa., software services company. "It is not our practice to discuss successes or failures," said Arthur A. Kock Jr., vice president and chief financial officer. [I guess potential customers just like their name?! -- RH]

The system is designed around four Prime Computer models known as Leopards, costing about $750,000 each. "Prime has had at least five people here full time trying to staighten things out," a bank official said. "This is going to be a really slick system, when it works," he added.

[Chickenfeed? BofA just declared a $1.14 Billion loss for the quarter on anticipated writeoffs for bad loans... PGN]

Computer crime, etc.

<Matthew_Kruk%UBC.MAILNET@MIT-Multics.ARPA>
Fri, 24 Jul 87 09:23:26 PDT

Speaking of computer crime, etc., it is timely that I noted the following article from Associated Press "buried" in our local paper:

Computer crime ring broken

Pittsburgh - Nine high school students in Pennsylvania have been arrested as part of a countrywide computer crime ring that illegally bought millions of dollars worth of goods and services, authorities say.
Juveniles and adults from New York City to California were involved, police said. The ring illegally obtained thousands of credit card numbers by using telephone hookups to tap the lines on which cards are checked

eletronically in many stores.
Illegal purchases of goods and services were made "in the millions," police officer John Michalec said Wednesday. More arrests are expected, he said.
Michalec said the ring also gained access to various government computers but he declined to elaborate "because of very delicate national security concerns that we don't want to talk about."

Computer crime, etc. -- and etc.

Peter G. Neumann <Neumann@csl.sri.com>
Sat 25 Jul 87 15:05:07-PDT

In the same week, two youngsters involved in the P.Floyd breakins at Stanford an Berkeley were apprehended on the west coast. Apparently the FBI and Secret Service have been trying to crack down on crackers. (See three articles by John Markoff in the SF Examiner, 23 and 24 July for background.)

Disclaimer: RISKS does not condone unsavory cracking, and certainly does not wish to glorify it. The systems that were broken into were not considered to be highly secure systems. However, we have noted here that even systems that are considered highly secure can be vulnerable to attack. On the other hand, we strongly urge emphasis on teaching that pervasively stresses social values and ethics as an integral part of education and life experience, not just on encouraging our youths to learn how to manipulate computers. PGN]

Reactor control-room design and public awareness (RISKS-5.15)

<ptsfa!rhc@Sun.COM>
Fri, 24 Jul 87 23:17:48 PDT

> This is regarded in several sectors as an increasingly sensitive subject,
> and I am of the growing opinion that it not appropriate to discuss
> this subject in an open forum. Readers should also note that several
> of the FORMER readers have included `experts' in this field.
> --eugene miya, NASA Ames Research Center

Eugene, Because it is an increasingly sensitive subject is exactly the reason it SHOULD be discussed. This is an open society, North, Poindexter, and the 'gipper' notwithstanding. If you don't want to express your opinions and share your knowledge about how to safely deal with the nuclear plants, then fine. I think this should be discussed so that we can know more about what may go wrong and how it happens. How else do you expect one to have an informed opinion? Osmosis??

(all standard disclaimers apply - your actual baud rate may vary,
depending upon atmospheric and cosmic disturbances)

Robert Cohen, San Ramon, California {ihnp4,lll-crg,qantel,pyramid}!ptsfa!rhc

[This is of course a very old debate in RISKS. In general, the awareness that there are serious problems is clearly a RISKS-related topic.

Considering the potentials for sabotage, misguided experiments, and so on there is a little justification for hiding the specific problems. However, if the existence of such problems is hidden, the public can be grossly misled. This debate thus echoes some of the Contragate hearings on what the public should know... RISKS always tries to opt for openness, while recognizing the sensitivity of certain details. PGN]

Computerized Tollbooths Debut in PA

Chris Koenigsberg <ckk+@andrew.cmu.edu>
Fri, 24 Jul 87 10:49:02 edt

The morning paper reported that new a computerized tollbooth system made its debut yesterday on the Pennsylvania Turnpike, at the King of Prussia/Valley Forge interchange (the exit for Philadelphia). It resulted in huge snarled traffic jams and delays.

Apparently they replaced the old toll cards, which you used to hand to the attendant who then asked for your fare, with new ones that you insert directly into a slot to be read by a computerized system which displays your fare on an LED readout. The new cards are so small, though, that no one can read them. So people didn't know what the fare was going to be until they saw it on the readout, whereas people used to read their card ahead of time and have their money ready.

Re: ATC Responsibilities (RISKS-5.15)

Alan M. Marcum <sun!marcum%nescorna@seismo.CSS.GOV>
24 Jul 87 18:35:17 GMT

In RISKS 5.15, Andy Freeman queried:
> What are the pilot's responsibilities and liabilities? What about the
> controller's?

The Federal Aviation Regulations are the laws governing aviation in the US. Subchapter F of the FARs is entitled "Air Traffic and General Operating Rules"; Part 91 of the FARs (part of Subchapter F) is entitled "General Operating and Flight Rules." FAR 91.3 states:

> 91.3 Responsibility and authority of the pilot in command
>
> (a) The pilot in command of an aircraft is directly responsible for, and is the final authority as to, the operation of that aircraft.

So, the PIC has total responsibility. 91.3 continues:

> (b) In an emergency requiring immediate action, the pilot in command may deviate from any rule of this subpart [91-A: General] or of Subpart B [91-B: Flight Rules] to the extent required to meet that emergency.

Yes, there is accountability for emergency deviations, under 91.3(c). (In fact, it's interesting to note that a large number of pilots have delayed declaring an emergency, or failed to declare an emergency altogether, because of this potential accountability. The FAA's official word -- and practice, from history -- is to declare the emergency, make the necessary deviations, and not to worry about "enforcement.") Regardless, this gives an idea of the authority of the PIC. Note that these regulations apply equally to all non-military flying in the US, air carrier, air taxi, and general aviation alike. As a (private) pilot, I take the accountability portions of FAR 91.3 very, very seriously.

Alan M. Marcum, Sun Microsystems, Technical Consulting, Mountain View, CA

[Also noted by John Allred <jallred@LABS-B.BBN.COM> and berry%solaria.s1.gov@mordor.s1.gov]

Air traffic control and collision avoidance

<willis@rand-unix.ARPA>
Fri, 24 Jul 87 15:39:06 PDT

Andy Freeman's comment in RISKS-5.15 and the ongoing discussion of ATC and related affairs prompts me to offer some historical perspective on the contemporary air traffic control system and anti-collision devices. Its history but it also has relevance to us as professionals in a computer world.

In World Wide II, an electronic radio-based technique called Identification Friend or Foe (IFF) was invented by the British. The problem at the time was to tell whether a radar-detected aircraft belonged to our side or to the other side. Successive generations of the system were designed and by the time it got to the one called Mark III, the various equipments in the system were brought to this country where everything was re-engineered and put into production for the Allied forces. The Hazeltine Electronics Corp, then of Little Neck, (Long Island) NY, was the focal point in the country for IFF work under USN contracts. Today we would call Hazeltine the systems engineering and support contractor.

The transponder gave a very simple reply to each interrogation pulse: a narrowly spaced pair indicating a normal response and a widely spaced pair indicating an emergency situation -- no identification of individual aircraft. In fact, there's a famous incident concerning the capture of several IFF equipments by the Germans from downed Allied aircraft; the foes flew in looking like friends and clobbered (I think it was) Bari, Italy almost into oblivion.

Toward the end of WW-II, the USN sponsored the design and development of a successor system called Mark V. Among other improvements, it transmitted a 10-bit response which could be coded to identify individual aircraft and operated at a higher frequency (L band) so the antennas could be smaller.

The war ended before Mark V got widely deployed and Hazeltine found itself

with all the great technology and ideas looking for a problem in the civilian world. Some internal studies were done and Hazeltine proposed a national air traffic control system which layered the airspace into 1000' increments (even altitudes going one way and odd altitudes, the other), put altitude-reporting transponders on all aircraft, assigned a unique identifier to each aircraft, and used ground interrogators to challenge the transponders. The responses were to be displayed on PPI scopes which also would contain correlated radar responses simply by synching the radar and interrogator transmiters. It was a very primitive digital system and naturally was to be done in vacuum tubes -- which is all there was at the time!

Then (1945-47) only the ENIAC had been built; the UNIVACs and the Princeton family of machines had yet to be developed. The digital computer had yet to really emerge so that the ground environment was not proposed to be highly automated.

Now to the point of this history. At the time, one of the important arguments, if not principle, was the question of responsibility. There were discussions about whether the pilots would accept a traffic control system that was ground based and would only give him directions. In fact, there were proposals to put the air picture together on the ground and transmit it back to the cockpits for decision making aloft.

All of the basic ideas in today's ATC were conceived, proposed, and implemented in the hardware-of-the-day some 40 years ago including the frequency assignments. The only conceptually new thing that has come along has been the computer-based automation that supports the controllers, although there has been of course a multitude of technology and engineering advances and the evolution of efficient operating procedures and overall system administration and some elaboration of the original basics. At the same time, the altitude-reporting transponder is a relatively recent addition; it roughly parallels the introduction of jet aircraft.

We all recall the slow progress of a ground-based ATC. Quite aside from the usual problems of introducing a new technology and persuading airline companies to put more equipment on aircraft (that, at the time, were generally weight, not volume, limited in carrying capacity), the pilots argued for having ultimate responsibility and decisions. For quite a while, we ran a national airspace with ground-based rotating light beacons, and various radio navaids. We didn't have radars, much less a transponder system.

Anti-collision proposals have followed the similar path; and for the same reason, we still don't have them in place except experimentally. One of the long running arguments has been the self-same "place of responsibility." The pilot, supported by his union and legal forces, has argued that the ultimate decisions had to be in the cockpit because of the legal responsibility mentioned by Andy Freeman. The electronikers of course argued that the job could be done much more effectively, efficiently, comprehensively, and cheaply on the ground.

Honoring the established wisdom of learning from history, there is something for our business. Namely, in the solutions and conceptual

frameworks that we propose for this, that, or the other application, we'd better be mindful of the legal environment in which the users of our systems will be; we'd better be especially sensitive to the legal obligations of the system users vs. where we put the automated support, how we funnel its output to the legally obligated users, and what legal responsibility it incurs.

It also relates to an aspect of compusec that has been little talked about; in fact I never recall it coming up in the defense environment although "2-man control" is a long established principle in stategic weapons control. It has come up only a little in the commercial compusec world although it's an implicit principle in traditional conduct of business in a paper world. It's "role separation" or division of responsibility.

Appropos of the insider threat and the overall integrity of system operation, there is a growing awareness that separation of role is an unaddressed but important latent issue in the compusec world. One shouldn't have the same individual both writing checks and signing them, nor should the implementation of a system allow an otherwise authorized user to have unauthorized access to both functions.

This principle also serves the reliability-of-performance issue. For some applications, notably ones involving high risk and/or public safety, one may be wise to separate the automated functions of monitoring and reporting from the (possibly automated or possibly manual) actual control of the process. But even then, we better watch the legal assignment of responsibility vs. the source of data on which to make decisions under that responsibility.

Willis H. Ware, Rand Corp., Santa Monica, CA

Risks of computerizing data bases

<@wiscvm.wisc.edu:T3B@PSUVM.BITNET "Tom Benson 814-238-5277">
Fri, 24 Jul 87 11:14:36 PDT

The following issue is a relatively one technically, I suspect, but may be fairly common. I am the co-author of a small book on nonverbal communication (Benson & Frandsen, NONVERBAL COMMUNICATION, Science Research Associates). For some time the book had a fairly large market as a textbook. Suddenly the sales fell off. Then my own university bookstore reported to me, when I tried to order it as a text, that it was out of print. I was pretty sure this wasn't so, and in a series of calls tracked down the answering/ordering service from which all college bookstores order the book. It turns out that the book was listed on the computer database under the name of the series of which it is a part (Modules in Speech Communication) and that occupied the title field; an attempt to request the title NONVERBAL COMMUNICATION returned a message that there was no such title, which the operator naturally interpreted by telling the bookstore there was no such title, so it must be out of print. So bookstores told this to professors, who ordered a different book. This first happened almost two years ago, and was followed by promises to correct it. It

happened again last week. It would seem that this is probably a fairly common situation, and that it is one that is very unlikely to reveal itself, since most people would not argue with the computer on such an issue. I'd be interested to hear whether such simple but mostly undetected errors (with real consequences in this case for the availability of this book) are common--and commonly corrected.

Re: electronic cash registers and wrong prices

<ucbcad!ames.UUCP!gatech!itm!brent@ucbvax.Berkeley.EDU>
Fri, 24 Jul 87 14:06:23 edt

Here in Atlanta, the Kroger stores advertise their "scan-rite" policy. That is, if any item gets rung up via UPC with a different price than that listed on the shelf, (and you catch them at it) you get that item free. This seems a reasonable policy in that "the punishment fits the crime."

brent laminack (gatech!itm!brent)

Re: Electronic Cash Registers

<blair%ncrwic%ncrlnk.dayton.ncr.com@RELAY.CS.NET>
Fri, 24 Jul 87 09:30:19 -0400 (at ncrlnk.Dayton.NCR.COM)

Michael Scott mentions an incident in which he was overcharged at a supermarket due to a discrepancy between the shelf price and the store computer's UPC database. The customer service desk expressed no sympathy, either.

Here in the Midwest we have a popular supermarket chain called Dillons whose president states (on the grocery sacks!) that he is so confident in his stores' computer/scanners (NCR) that he guarantees that if an incident similar to Mr. Scott's occurs, the customer receives the disputed item for free. Not a bad idea!

Brian R. Lair NCR Corporation, E&M Wichita, Product Technology Development
<brian.lair@Wichita.NCR.COM>
<{ece-csc,hubcap,gould,rtech}!ncrcae!ncrwic!brian.lair>

Re: Electronic cash registers

Will Martin -- AMXAL-RI <wmartin@ALMSA-1.ARPA>
Fri, 24 Jul 87 10:21:49 CDT

The RISK to the public of incorrect computer-controlled grocery-store pricing may be the most common form of computerized fraud perpetrated on the general populace. At least, I think it is the most likely to happen to the ordinary individual.

The inconsistency between shelf-posted prices and what the stores' computers have as the on-line price is still fairly common around here (St. Louis); more likely at National stores, which is one of the two chains I normally shop at. When scanning came in and individual-item price-marking was dropped, there was much publicity about how the stores would give you your money back if you were charged more than the shelf price. These policies are still in effect, but are not publicized any more. Also, I think the staff have gotten so used to the system that they have become sloppy and careless.

I often get several dollars' worth of free groceries by remembering what the shelf price is and watching the display during checkout. You just pay what the register shows, and then take the ticket and items to the manager's cubicle and point out the discrepancy. The way the refunds are implemented now is that, if you bought more than one each of an item where the price was wrong, you get one free and a refund for the difference on the others. If you bought one each of several items where the prices were wrong, you get all the cost refunded (plus you get your sales tax back, too, of course). One interesting aspect of this is that the local stores have been doing "double coupons" for the past year or two -- if you had redeemed a coupon on the item, they are paying you twice the coupon value to take the thing! (Only once did the manager check on coupons and give me back the coupon and cancel out its redemption and adjust the refund accordingly.)

This is actually cheaper for the stores than trying to do it right in the first place, I think. They are paying me by giving me free groceries to do their job for them; since probably only a tiny fraction of the great unwashed consuming public pays close enough attention to what they are doing to catch these price discrepancies, it doesn't really cost the stores that much -- undoubtedly cheaper than it would cost to pay their staff high enough wages to expect them to be more accurate all the time! Plus, of course, they get the extra income from overcharging the majority of customers until they are caught.

The stores also have an interesting method of correcting the discrepancy: they never change the computer price -- they just change or remove the shelf tag! (At least I have never seen any evidence that the computer-stored price gets changed.) When you report the discrepancy to the manager, they send a stockboy to pull off the shelf tag.

This sort of thing can be consistent and repeatable, too -- for example, there is a local brand of taco chips I only buy when they are on sale for 99 cents a bag istead of the usual $1.29, and EVERY time I buy these I get a free bag! The store seems to never change the computer price when they put up the "sale" sign on the chip display! (Usually I buy these on Monday, the first day the new price would be in effect, but I have run into this as late in the week as Wednesday evening. That means that three days' worth of shoppers have not yet noticed the price difference, in a huge busy store, or the computer price has not been updated despite reports.)

Anyway, if you are alert enough to pay attention, this is one RISK that you can turn to your advantage.

Regards, Will Martin

---

supermarket scanner errors

<fulk@cs.rochester.edu>
Fri, 24 Jul 87 14:29:55 EDT

[Note to risks readers: Michael Scott and I are colleagues in Rochester. Topps and Wegmans are the largest of the local grocery chains, and the main representatives of the hypermodern gigantic school. Topps goes for the blue-collar clientele; Wegmans is ritzier.]

Topps or Wegmans? We always have this problem at Topps, and average about 25 cents a trip or so in scanner errors. We check the receipt very thoroughly every time; I'll go back in the store and recheck shelves to be sure. They are always very nice about giving us our money.

At Wegmans, on the other hand, you get the item free, or a dollar back, whichever is less. One used to get the entire order free at Wegmans for catching a scanner error; from the fact they stopped, I gather that other people than I noticed the following obvious strategy: buy one copy (at least) of every item in the store; one item is sure to scan wrong, so you will get the entire order free. Out of some undoubtably foolish sense of rightness, I never tried this; however, I did get several free normal orders for noticing scanner errors. The change in policy has caused me to switch to Topps, which has generally lower prices. I just have to be more watchful.

Please to note that the number of scanner errors is substantially smaller than the number of errors committed by clerks at manual cash registers; furthermore, the scanner errors are much more easily checked, since each line of the receipt shows the item scanned. I have only caught one error in interpreting the bar code.

Mark

[I have omitted a slew of additional messages on this subject, some of which are worthy but others of which are rather chatty. It is hard for me to accept just a novel portion of a long message. RISKS usually gets deluged on issues that affect us personally, particularly in the wallet. PGN]

Taxes and who pays them

<Rick.Busdiecker@h.cs.cmu.edu>
24 Jul 1987 05:54-EDT

Unfortunately the clarification is not entirely correct, although it is fairly widely held misbelief. While the application of a new tax to a product or service will often result in an increase in cost to the end user, it is very often NOT the case that this end user cost increase is equal to the tax increase; in many cases the company absorbs some of the cost. A government decree will not necessarily affect the price

that a market will bear in as predictable a manner as is suggested by this ``clarification.''

Rick Busdiecker

Non-taxes and who pays them [For the record]

Andrew Klossner <andrew%lemming.gwd.tek.com@RELAY.CS.NET>
Sat, 25 Jul 87 11:22:20 PDT

Two recent comments in RISKS have suggested that the FCC is levying a new tax on data transmission. This is not the case. In fact, the FCC has proposed to discontinue a telephone service discount that information service providers now enjoy. The effect on those service providers is the same, but the government motivation is a bit more noble than just grubbing for new revenue.

-=- Andrew Klossner (decvax!tektronix!tekecs!andrew) [UUCP]
(andrew%tekecs.tek.com@relay.cs.net) [ARPA]

[Thanks for the clarification on this. As we have drifted from RISKS relevance, let's blow the whistle on this subject. PGN]

Search RISKS using swish-e

Report problems with the web pages to the maintainer

Search RISKS using swish-e

THE RISKS DIGEST

Forum on Risks to the Public in Computers and Related Systems

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

Volume 5: Issue 17

Sunday, 26 July 1987

Contents

Re: Separation of Duties and Computer Security

Ted Lee <TMPLee@DOCKMASTER.ARPA>
Sun, 26 Jul 87 12:42 EDT

It is not true that development of computer security principles in the "defense establishment" has ignored the principle of separation of duties. At class B2 of the Orange Book a system is required to support separate operator and [security] administrator roles. At B3 and above it is quite explicit that a) to assume the security administrator role a distinct auditable action must be taken, and b) that when performing in that role a person is limited to ONLY doing those things "essential to performing the security role effectively." Furthermore, there was quite a long discussion at one of the recent national conferences (I forget whether it was the last Oakland conference or the NBS/DoD before it) about the topic of separation of duties as found in the financial community and how it did or did not relate to the kinds of security policies "traditionally" found in trusted systems. One could in fact argue that the fundamental principle of "need-to-know" versus "clearance" is a kind of two-man rule: the person who decides to let me see a particular classified document, based on his judgement that I need to see it, is not the same person who grants me the clearance that I must have in the first place.

Re: Robocop (RISKS DIGEST 5.12)

Zalman Stern <zs01+@andrew.cmu.edu>
Sat, 25 Jul 87 22:23:22 edt

On the one hand, I am loathe to assign any sort of serious meaning to Robocop. It was basically lots of very well done violence with a streak of humor thrown in. The most thought provoking question I had after seeing it was "Who in their right mind would trust anything that carried a big gun and ran MS-DOS?" On the other hand, Ebert's quote clearly ignored the major plot line of the movie. The guy who was championing ED-209 (The robot that gunned down a board member during a demonstration) really didn't care if it killed people. One of his quotes was something to the effect of "I had it all lined up. Millitary contracts, spare parts for the next 25 years. The profits would have been great. Who cares if it worked!" Of course the competition for the ED-209 was a cyborg (half human) which had human judgement and therefore was much safer... The other great social comment in the movie was the not-so-overdone "trivialize death and suffering" newscasts.

As for computer risks, there was one lesson to be learned from Robocop. If you are going to program back doors into an armed robot to protect yourself, make sure you word your logic strongly enough so you don't get blown away in the end :-)

Zalman Stern, Information Technology Center, Carnegie Mellon University
Pittsburgh, PA 15213-3890
Internet: zs01+@andrew.cmu.edu Usenet: ...seismo!andrew.cmu.edu!zs01+

Re: B of A's computer problems

Bob Larson <blarson%castor.usc.edu@oberon.usc.edu>
26 Jul 87 04:17:56 GMT

In article <8707252233.AA15919@csl.csl.sri.com>:
>The system is designed around four Prime Computer models known as Leopards,
>costing about $750,000 each. "Prime has had at least five people here full
>time trying to staighten things out," a bank official said. "This is going
>to be a really slick system, when it works," he added.

A couple of corrections: The "leopard" was Prime's development name for the 6350. B of A did not have any in March, since the 6350 had not been announced and B of A was not a hardware beta test site. (USC was one of three beta sites for the 6350, ours was installed in April if I remember correctly.)

(Chances are that B of A got 9955-II's and planned to upgrade.)
Bob Larson Arpa: Blarson@Ecla.Usc.Edu
Uucp: {sdcrdcf,seismo!cit-vax}!oberon!castor!blarson

Southern Methodist University <Leff>
Sat, 25 Jul 1987 19:56 CST

<E1AR0002%SMUVM1.BITNET@wiscvm.wisc.edu>
Subject: Nuclear power plant monitoring and engineering
To: RISKS%CSL.SRI.COM@RELAY.CS.NET

Attached, please find some references to applications of computers to nuclear power plant monitoring and engineering. A frequent theme is to try and reduce cognitive overload in the event of a critical situation, i.e., present something other than 500 alarms ringing at once.

Works in the control engineering field address this issue in a more general context: power plants, nuclear plants, chemical plants etc. A couple of AI based tools for fault tree analysis which is used in estimating risk probabilities in the nuclear field among others have also been announced at various conferences.

For those desiring to track this field, you should watch the American Control Conference every year and the section for nuclear engineering and control engineering in the IEEE Computer and Control Abstracts. This is very complete: our librarians complain that people keep requesting references from there that are not in any library in the United States which makes Interlibrary Loan a tad bit difficult. It ranges from six months to a year behind the date of publication unfortunately for the printed edition.

As far as the RISK of an accident, the average number of days of life loss for nuclear accidents in the United States is on the order of two days per person. This uses probabilities estimated by antinuclear power plant groups. The number of days lost is a tenth to a hundredth of such risks as automobile accidents, lighting and the like which we accept on a regular basis.

Hans Mark pointed out that the loss of life from Chernobyl due to delayed cancers would be lost in the "noise." That is no statistical test done on deaths in the Soviet Union could discern that something happened. If nuclear power plants were removed and replaced with coal burning plants, more people would die from the radiation released into the atmosphere by the burning coal. This ignores the death toll from coal mine accidents and air pollution. In short nuclear power plants are about as risk free as one can get in this society and our energies are much better off being devoted to automobile accidents, cigarrette smoking and alcohol addiction.

[Following is left as is for UNIX users. Apologies to others. PGN]

Sachs, P. A., Paterson, A. M. and Turner, M. H. M., Escort - An Expert System for Complex Operations in Real Time,
\fIExpert Systems\fR, Vol. 3, No. 1, pages 22-28, January 1986.
.P2
Describes a system to assist operators in controlling such systems as off shore oil rigs and nuclear power plants. It works by reducing the number of alarms and hence the operator's cognitive overload.

Faught, W. S., Applications of AI in Engineering,
\fIComputer\fR, Vol. 19, No. 7, pages 18-27, July 1986.

.P2
Discusses applications of KEE to diagnosis of the Space Station Life Support System and satellites, simulation of factory cells in sheet-metal manufacturing, and determining the best fuel shuffling for a nuclear power plant so as to keep the shutdown costs as low as possible.

Underwood, W. E.,
A CSA Model-based Nuclear Power Plant Consultant
In \fIProceedings 2nd NCAI\fR, pages 302-305, Pittsburgh, August 1982.
.P2
The Common Sense Algorithm representation is used to model the physical system. Diagnostic rules are also represented in this formalism.

Nelson, W. R.,
REACTOR: An Expert System for Diagnosis and Treatment of Nuclear Reactor Accidents
In \fIProceedings 2nd NCAI\fR, Pittsburgh, pages 296-301, August 1982.
.P2
REACTOR is being developed at EG & G, Idaho, for assisting operators in the diagnosis and treatment of nuclear reactor accidents.

Ancelin, J. and Legaud, P., An Expert System for Nuclear Reactor Alarm Processing
In \fISixth International Workshop on Expert Systems and Their Applications\fR, Avignon, France, April 28-30, 1986.

Piette, D., Roche, C. and Ianeselli, J. C., ALPA: Diagnosis Expert System for Supervision of Nuclear Reactors In
\fIECAI '86. Seventh European Conference on Artificial Intelligence (Brighton, England)\fR, Vol. 2, pages 109-113, July 1986.
.P2
The use of an expert system to monitor and diagnose nuclear reactor breakdowns. Various knowledge representation schemes were tried.

Hoernes, P. E., Salame-Alfie, A. and Yeater, M. L.,
Enhanced Inspection of NPP's Using Expert Systems as a New Approach,
\fITransactions of the American Nuclear Society\fR, Vol. 53, pages 275-277, 1986
.
.P2
The development of a small expert system in evaluation of nuclear power plant performance as part of the process of inspecting it.

Corsberg, D., Extending an Object-Oriented Alarm-Filtering System
In \fIExpert Systems in Government Symposium\fR, McLean, Virginia, pages 80-87, Oct. 22-24, 1986.
.P2
This system uses functional relationships as opposed to fault/consequence trees to provide necessary alarm filtering in a nuclear power plant.

.P1
Brodsky, S. and Tyle, N.,
Knowledge-based Expert
Systems for Power Engineering
In \fIProceedings of the

15th Pittsburgh Modeling and Simulation Conference\fR, Pittsburgh,
April 1984.
.P2
Paper presents a brief review of the development and application of expert systems in areas related to electric power engineering. The specific examples discussed include nuclear power plant monitoring, power system restoration and hydro-electric plant design. In addition, several problems are examined as candidates for future expert systems.

%A Mark A. Fischeti
%A Glenn Zorpette
%T Power and Energy
%J IEEE Spectrum
%V 23
%N 1
%D JAN 1986
%K AA04 AI01 Westinghouse Electric Corporation nuclear power Babcock and Wilson EG&G Idaho reactor
%X "Westinghouse Electric Corporation of Pittsburgh, PA offers the Genaid diagnostic software package to monitor changing conditions in power plant generators, analyze them, and warn plant operators of potential trouble." EG&G Idaho of Idaho Falls has a Reactor Safety Assessment system which "processes large amounts of data from a nuclear power plant during an emergency, makes diagnoses, and outliens the consequences of subsequent actions. After final refinements, this expert system program is to go on line this year at he Nuclear Regulatory Commison's Operations Center in Washington Center. The system was developed for use with Babcock and Wilcox Pressurized-water reactors and will be adapted for use with other reactors." [In Spang-Robinson report, they indicated that the Japanese are putting major amounts of money into expert systems for nuclear reactor operations. See my summary for more info. LEFF]

%A D. Sharma
%A B. Chandrasekaran
%A D. Miller
%T Dynamic Procedure Synthesis, Execution, and Failure Recovery
%B Applications of Artificial Intelligence in Engineering Problems
%E D. Sriram
%E R. Adey
%V 2
%I Computational Mechanics Publications
%C Woburn, Massachussetts
%D 1986
%P 1055-1072
%K AA05 nuclear power plant AI01 AI09
%X Describes a system for planning failure recovery, synthesis, monitoring for nuclear power plants. A comparison of the "event-oriented" and "function oriented" approaches to nuclear power plant management is provided. The nuclear industry is shifting to the latter in reaction to the TMI difficulties. The implications of this for expert system applications and an example from reactor scram concerns are also provided. Various plan templates and blackboards are used in processing. The final expert system consists of system specialists, specialists in various kind of undesirable

events and specialists in various kind of goals such as reducing radioactivity.

Search RISKS using swish-e

THE RISKS DIGEST

Forum on Risks to the Public in Computers and Related Systems

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

Volume 5: Issue 18

Monday, 27 July 1987

Contents

Its Barcode is NOT worse than its Byte; Rooting for AT&T PC truffles

Elizabeth Zwicky <zwicky@tut.cis.ohio-state.edu>
Mon, 27 Jul 87 11:27:38 EDT

Two security notes:

First, on the discussion about scanner errors in grocery stores. The chance that these are actually scanning errors is so small as to be ignorable. The UPC barcode they use is incredibly reliable, and includes two separate check digits encoded in different ways. What is very likely to go wrong is the shelf labels. Usually, the system is that the computer database is updated, and automatically prints revised shelf labels. There then is a considerable

lag while the labels are actually put on the shelves. Of course, sometimes they forget to update the database, especially for sales.

Second, on actual computer security. We have 40 AT&T PC7300s that are used to teach an introductory computing course. We have had notable problems with them (our current favorite causes students with output loops to end up losing the lab they're working on, source code and all), but were surprised when the root passwords started to mutate. One of us asked the monitor in the lab, who offered to break root for him so he could change it back. It seems that with two mouse clicks, and two presses of the enter key, you can get a root shell. There's a bug in the shutdown procedure, causing it to give you all its warnings, push a root shell (complete with window system that says "Office of root", just in case you don't know you're root), and then stop. Most of the students don't know enough about UNIX to make any use of this trick, but some of them seem to find changing the passwords around amusing.

Elizabeth Zwicky

[Suns reportedly have a similar feature! PGN]

Too much security?

Richard Schooler <schooler@inmet.inmet.com>
Mon, 27 Jul 87 11:48:12 EDT

A mainframe system that we have occasion to use retires passwords every 28 days and does not allow any of the four previous passwords to be re-used. Since we use the system mainly for re-hosting (i.e., not "real" work or personal files), the onerousness of this scheme has driven many of us to using extremely easy-to-remember passwords on that system, such as the name of the current month. I find this quite ironic.

Richard Schooler, Intermetrics, Inc. {ihnp4,ima}!inmet!schooler

[This is an old RISKS problem, but worth including for newer readers. PGN]

"Hacker Program" -- PC Prankster

Sam Rebelsky <r032@sphinx.uchicago.edu>
Mon, 27 Jul 87 11:23:22 cdt

I thought people might be interested in a small article that appeared in a sidebar of today's Chicago Tribune, Business Section, Monday, 27 July 1987.

"You'd better watch out

A new software program lets anybody with access to an IBM or IBM-compatible personal computer become a hacker, at least on a small scale. The program, from Mainland Machine, San Luis Obispo, Calif., is called PC-Prankster.

It wasn't necessarily designed with the idea of making the world a better place in which to live. An electronic jokester can sneak up and install PC

> Prankster on a friend or loved one's ``boot disk,'' (the disk used to fire up
> the computer's operating system when it is turned on), whereupon it resides
> in memory waiting for its chance to pounce.
>
> As soon as the PC user reaches a certain set number of keystrokes, the
> prankster takes over. The work in progress disappears, one of five ugly
> creatures fills the screen and blows a kiss, then vanishes, and the screen
> returns to where it was before the intrusion. The prank repeats itself
> every 5 minutes or so.
>
> Among the characters are a cyclops that blinks and a flasher that flashes.
> The only way to get rid of PC-Prankster is to use the delete program
> contained on the disk. Or you could drop your PC out the window, timing
> it to land on the perpetrator. PC Prankster costs $19.95 and also works
> on hard disk systems.

This really bothers me. The article (and the program) imply that fooling with someone's work on a computer is acceptable and that hacking is just harmless playing. The article also seems to imply that the program is otherwise harmless "..and the screen returns to where it was before the intrustion." I find it unlikely that such a program will be perfectly harmless in all cases.

I'm sure other people are more qualified to comment on other risks of such a program, including the similarity of such a program to a trojan horse.

SamR

Pittsburgh credit card hackers

Chris Koenigsberg <ckk+@andrew.cmu.edu>
Sun, 26 Jul 87 23:54:50 edt

In RISKS 5.16, someone mentioned that a ring of teenaged credit card hackers was recently broken. What they didn't mention is that the solving of the case had nothing to do with the computer end of it at all. One of the kids bought a skateboard with a hot card number, and his mother was so annoyed at his use of the skateboard that she turned him in!

[The wheels of (mis)fortune! PGN]

Hacking and Criminal Offenses (Re: RISKS 5.15)

David Sherman <mnetor!lsuc!dave@seismo.css.gov>
Mon, 27 Jul 87 12:36:32 EDT

> > The dishonest obtaining of access to a computer data bank
> > by electronic means is not a criminal offence.
> >
> >Under the terms of the Act, Gold and Schifreen were charged with "making
> >a false instrument on, or in, which information was recorded or stored by
> >electronic means, with the intention of using it to induce the Prestel

>computer to accept it as genuine, and by reason of so accepting it to do
>an act to the prejudice of British Telecom plc".

This case is reminiscent of the Supreme Court of Canada decision in R. v. McLaughlin (1980), 113 DLR(3d) 386-394. In both cases the authorities attempted to use a statute enacted for other purposes to prosecute unauthorized computer use.

In the British case, as outlined above, the Act used was one which makes forgery and counterfeiting illegal. In the Canadian case, which involved a University of Alberta student obtaining unauthorized access to a university computer, the charge was that of fraudulently using a "telecommunication facility", in violate of s.287 of our Criminal Code. (That provision is the one used for people who use blue boxes to make long-distance calls.)

The Supreme Court's decision boiled down to this quote (at p. 394):

> Had Parliament intended to associate penal consequences the unauthorized operation of a computer, it no doubt would have done so in a section of the Criminal Code or other penal statute in which the term which is now so permanently embedded in our language is employed.

The result was that Parliament did indeed enact legislation making illegal the unauthorized use of computers (in 1986). It looks like the British Parliament will have to do the same. In the context of the quote above, the decision of the English Court of Appeal is probably correct. I'll be interested in seeing whether the Court of Appeal referred to the (Canadian) McLaughlin case.

David Sherman, The Law Society of Upper Canada, Toronto
{ uunet!mnetor pyramid!utai decvax!utcsri ihnp4!utzoo } !lsuc!dave

---

911 Surprises

Paul Fuqua <pf%islington-terrace%ti-csl.csnet@RELAY.CS.NET>
Mon, 27 Jul 87 14:30:54 CDT

Tarrant County (Fort Worth) is about to start a 911 emergency telephone service, the second in the state, prompting quite a few newspaper articles about aspects of their service and that of Harris County (Houston), which started in January 1986.

The details I found most interesting were the problems that had to be overcome in both systems. (Quoted without permission from the Dallas Morning News)

> For instance, Harris County found initially that people dialing a seven-digit number with 911 in it would sometimes reach the emergency operator by mistake. Telephone company computers were so quick, they would pick up the 911 and transfer the call before waiting for a fourth digit. [There are no other magic three-digit calls in this area: for 411, one dials 1411, and all other numbers are seven digits. - pf] ...

> In the beginning, 911 operators were deluged by calls from children trying out the system and from people who put the 911 number on the speed-dialing function on their telephones and hit the number by mistake.
>
> Misdirected calls also come in from cordless phones whose batteries are low -- a situation that seems to mistakenly trigger calls to 911 ...
>
> Another problem Tarrant County is working on is establishing street addresses for rural homes. The [911] district is working with the U.S. Postal Service and telephone companies to assign street addresses to more than 9,000 locations in Tarrant County so that a recognizable address will appear on the screen -- not just a rural route and box number.
>
> [The director] was surprised when the effort met some resistance. ... "Some people have said, `I'm not going to use 911 so I don't need my address changed.'"

Tarrant County will start up their system on August 2, despite the failure of equipment to automatically transfer the address information from the emergency operator to the appropriate agency. Dallas County (Dallas) expects to start their own service next April; the goal is that the whole state will have 911 by 1995.

Paul Fuqua, Texas Instruments Computer Science Center, Dallas, Texas
CSNet: pf@ti-csl UUCP: {smu, texsun, im4u, rice}!ti-csl!pf

Re: Taxes and who pays them (RISKS DIGEST 5.15)

<cew@venera.isi.edu>
Mon, 27 Jul 87 11:19:18 PDT

This idea of "passing it on" is nonsense. A Company, or any organization selling a product or service, will charge as much as it can for its product or service. It does not matter how much the product costs them or how much it is taxed or how much of the external costs are forcibly internalized by regulations. The question is simply "Does the amount received sufficiently cover the cost of production to justify the organization continuing the process?" If the profit is too small or non-existent then the process is halted. If the profit is great, others will get into the act.

For the topic that came up in Risks, the question is "How will the companies providing electronic communications services respond to the added costs of FCC taxes?" Some possible responses are (1) absorb them (not bloody likely), (2) Add them to the price for the service (not a "passing on" but a shift in customer base), (3) Absorb them for a while and add them slowly to see how the customers react and (4) Get the FCC changed.

In my view, the key result of this will be to shift the customer base away from private individuals to corporate individuals (corporations can more easily add the extra costs to their products). My question is then "Why is the FCC using its taxing privileges to manipulate the electronic

communications market to force out the private individual?" That leads us away from the risks of computers to risks of another kind.

(If people want to argue this view of economics they should send mail to me directly. No need to clutter Risks with these more general questions.)

Craig

Statistics as a Fancy Name for Ignorance

Mark S. Day <MDAY@XX.LCS.MIT.EDU>
Mon 27 Jul 87 13:32:55-EDT

The risk-assessment numbers put forth to justify nuclear power's safety remind me of Mark Twain's observation that there are three kinds of lies: lies, damned lies, and statistics. What real evidence or experience do we have for these projections and statistics? How can we meaningfully discuss the "safe" containment of wastes that are dangerous for a time span comparable to all of recorded history so far? How much do we really know, and how much of it is based on "plausible" guesses and conjectures?

The fact that nuclear power plants have been run in a generally safe way in the past tells me very little about the future danger from them. Predicting the future like that is similar to the statistical fallacy that if a fair coin has come up "heads" 500 times in a row, it is somehow "more likely" to come up "heads" the next time that I flip it. [Alternately, some people also believe that it's "more likely" to come up "tails", since it's "about time".]

Car wrecks and cigarette smoking kill more people than nuclear plants, sure, but the way that they kill people is very different. Car accidents generally don't affect a zone of several miles' diameter, forcing evacuation and abandonment of homes. Cars and cigarette smoke are perceptible, whereas radiation isn't (I know that carbon monoxide is odorless and colorless, but you rarely get carbon monoxide from cars or cigarettes without smelly components, too.). Chernobyl has shown that when an accident occurs, it doesn't matter that it's a rare event: it's an extremely unpleasant event. Who cares if a meltdown happens "once in 100,000 years" if it happens tomorrow? It is perfectly rational to decide that a potential catastrophe is undesirable, no matter how rare it is.

--Mark

Supermarkets

Chris Koenigsberg <ckk+@andrew.cmu.edu>
Sun, 26 Jul 87 23:59:38 edt

The Giant Eagle chain of supermarkets in western Pennsylvania has automated checkout scanners at the bigger stores. But they also have a policy they call Absolute Minimum Pricing, and as a part of this, they have a strict rule that you can be ejected from the supermarket if you are caught writing down their prices from the tags on the shelves (because they want to keep the jump on

the competition)! So I suppose very few people ever manage to catch scanner price errors at Giant Eagles.

[This is an interesting new twist. PGN]

Grocery store scanners and shelf tags

Jon Mauney <mauney@ece-csc.ncsu.edu>
Mon, 27 Jul 87 09:54:45 EDT

Don't forget the Hi-Tech creed:

What is fouled up by technology can be fixed by further technological patches.

In the case of computerized cash registers, help is on the way in the form of radio-updated LCD shelf tags. (This is according to an article in last week's Sunday News and Observer. I can dig it out, but it is unlikely to contain any useful facts.)

Of course, this will bring two new risks:

The price may go up while you're waiting in line.

The tags may be affected by teenage vandals who have gotten bored with breaking into computers.

Jon Mauney

[Recalling the students who spliced themselves into the comm line to the Rose Bowl scoreboard and took over the display, we can certainly look forward to someone changing the prices downward just before checking out. PGN]

Search RISKS using swish-e

THE RISKS DIGEST

Forum on Risks to the Public in Computers and Related Systems

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

Volume 5: Issue 19

Wednesday, 29 July 1987

Contents

Automating Air Travel

Dan Graifer <sdcsvax!net1.UCSD.EDU!graifer@ucbvax.Berkeley.EDU>
Mon, 27 Jul 87 16:49:18 PDT

In The Economist, July 25, 1987, pp. 73-74, there is an interesting look at the coming automation of commercial airports. Deregulation has led to explosive growth in demand, with consequences all of us who fly can talk at length about. The chart in the article shows the current ~10^12 revenue passenger miles/year almost doubling by the year 2000.(~6% growth per year).

The article discusses the introduction of automation to cope with increasing airport and aircraft size. After a brief look at automated ground traffic control, including arrival gate assignment, it concentrates on evolving mechanisms for baggage sorting and handling. There is also a brief mention of the problems associated with sharing ticket counter facilities by small

airlines when each uses a different, incompatable, reservation system. Large emphasis is placed on a new International Civil Aviation Organisation rule effective next year that will require carriers to match every piece of baggage loaded with a passenger verified to be on the aircraft.

In addition to a brief survey of the technologies involved, there is a lot of discussion of the potential problems: Simple system breakdown, incompatible tag systems at different airports, accidental mischief (child with toy magnet scrambling magnetically encoded tickets), and malicious mischief (as simple as disgruntled employees entering false gate data, thereby running aircraft around in circles).

My favorite "fun" prospect mentioned is baggage tags where the human and machine readable destinations differ... This one reminds of the old check kiting scheme based on checks with mismatched bank name/numbers.

The article is very witty, and I just hope the people designing these systems are experienced. I think we can find examples of just about every kind of risk ever mentioned in this forum lurking here.

Oh yeah, the solution to the incompatible reservation system problem is CUTE...Common Use Terminal Equipment.

Dan Graifer

Responsibilities of the pilots and the traffic controllers

Nathan Meyers <hpda!hp-pcd!hpcvra!hpcvrp!nathanm@ucbvax.Berkeley.EDU>
Mon, 27 Jul 87 17:29:47 pdt

In RISKS 5:15, Andy Freeman asked, in regard to commercial airline operations:

> What are the pilot's responsibilities and liabilities? What about the
> controller's?

As one of many private pilots reading RISKS, I'll try to answer. In so doing, I will attempt to simplify the system enough to a) be understood by non-pilots, b) not insult too many pilots, and c) not reveal too much of my own ignorance.

The statement of the pilot's responsibilities is, like the U.S. constitution, very succinct and, also like the constitution, full of implications:

The pilot-in-command is responsible for all aspects of the flight.

Among other things, this means:

1) The pilot can refuse Air Traffic Control (ATC) instructions.

2) Whatever the co-pilot, navigator, flight attendants, airline executives, controllers, and everyone else have to say, it is the pilot who has the final word on whether a flight is go or no-go.

3) No matter who's being paid to de-ice the wings, fill the gas tank,

> inflate the tires, clean the windshield, etc., it is the pilot's
> responsibility to determine that the aircraft is ready to fly.

What are ATC's responsibilities? To put it very succinctly (probably too succinctly):

Advisory, sequencing, and separation.

This, of course, means a lot of different jobs. These jobs are handled by four different parts of the ATC system which usually involve different personnel and, somehow, intermesh, communicate, and coordinate. These four pieces (not found at all airports) are:

1) Ground control (take care of traffic on the ground up to the runways),

2) Tower (control use of the runways, specifically through takeoff and landing clearances),

3) Approach and departure control (control air traffic in the vicinity of the airport), and

4) Enroute traffic control (control air traffic everywhere else).

Ground control and tower operations take place in a tower with a view, approach/departure control takes place in a darkened room full of radar scopes, and enroute traffic control takes place in a darkened room at a regional center (for example, a center in Seattle watches over most of the Pacific Northwest).

During the course of a typical flight under Instrument Flight Rules (IFR), ATC tells the pilot when to taxi, when to take off, when to ascend and descend (and to what altitudes), when to turn, and when to land -- all based on a flight plan filed by the pilot. The pilot's job is to worry about which way the aircraft is pointed and what's going on in its vicinity -- ATC's job is to allow lots of aircraft to use the same airspace (clouds and all), airports, runways, and terminals. That, in a nutshell, is my attempt to answer Andy's question.

So what's gone wrong with the system?

There's been no shortage of finger-pointing. Some blame general aviation (little guys like myself), some blame the PATCO strike, some blame drugs, some blame deregulation, some blame pilot training.

The answer, of course, isn't all that simple -- it involves economics, politics, technology, the Reagan military buildup, personnel, unions, etc. So far, nobody in any position of power has come up with any solution more creative than to increase regulation of the already heavily-regulated airspace.

My own pessimistic prognosis is that the air traffic system has a lot worse to get before it's going to get better.

Nathan Meyers (hplabs!hp-pcd!nathanm)

[We have noted Henry Petroski's evidence that we tend to learn little from our engineering successes, but that the real advances come from trying to understand our failures. There is MUCH to be learned from the ATC situation, especially when confronted with the realization that many of the existing problems will continue to exist even when the long awaited new computer systems arrive. PGN]

Flippin' statistics

Joe Morris (jcmorris@mitre.arpa) <jcmorris@mitre.arpa>
Tue, 28 Jul 87 11:16:13 EDT

In RISKS 5:18, Mark Day writes:

> The fact that nuclear power plants have been run in a generally safe way in
> the past tells me very little about the future danger from them. Predicting
> the future like that is similar to the statistical fallacy that if a fair
> coin has come up "heads" 500 times in a row, it is somehow "more likely" to
> come up "heads" the next time that I flip it.

Sorry, but that's true only if you assume that the coin is balanced to have equal probability of falling heads or tails. A balanced coin would have a probability of 2^-500 of 500 consecutive heads; while not impossible, a run of that length would lead a reasonable person to conclude that the coin was balanced in favor of heads. I suggest that the nuclear power industry is still demonstrating a good track record and will probably continue to do so. This doesn't say that there won't be a disaster, but if you want to dismiss the operating history, you should explain why it represents a statistical anomoly. (Coverup, progressive deterioration, etc.) After 500 consecutive heads, it isn't unreasonable to expect a 501st head as well.

On the other hand, it is perfectly reasonable to consider whether the potential damage from an accident outweighs the small probability of its occurrance, or whether it is outweighed by the reduction in consumption of non-renewable fuels. Unfortunately, the analysis may be technical, but the decision will be political.

Nuclear power safety and intelligent control

Whitewater Wombat <rsk@j.cc.purdue.edu>
Tue, 28 Jul 87 21:48:05 EST

In RISKS-5.14, Alex Bangs raises two concerns relating to nuclear power plant safety (construction corruption, intelligent control systems) and requests references on nuclear power plant control.

Let us assume, for the sake of argument, that a given plant may be constructed without "corruption"; I interpret that to mean that the plant is built exactly to specification. Such a procedure does not guarantee that the specification itself is correct; nor does it guarantee that a properly constructed plant built to a correct specification will continue to adhere to that specification

after it is put into operation. I do not mean to de-emphasize the problems that result from shoddy construction practices, but merely to point out that these are not the only problems; perhaps they are not even the major ones.

With regard to the use of intelligent control systems, a similar plethora of problems exist. Although [hopefully!] intelligent control systems known as "human beings" are now used to operate plants, the multitude of sensor inputs (some of which may be erroneous) and the large number of possible failure modes pose problems that are exceedingly difficult to solve even when copious time is available--which it sometimes isn't.

Consider also what repercussions have already occurred for the nuclear industry as the result of [possible] human error during crisis situations; now imagine the outcry if the public at large discovered that a nuclear accident occurred in part because of a fault in an expert system---a "computer error".

Two excellent references on the subject are:

IEEE Spectrum Vol 16 #11 Nov 1979 and Vol 21 #4 Apr 1984

Both issues cover TMI extensively, especially the first. They are eminently readable to anyone with a technical background; I believe the first issue won a number of awards for its coverage.

Finally, a brief anecdote. On March 28, 1979, I was in St. Louis for an interview with Union Electric Co. for a possible position at their then-under-construction nuclear facility at Callaway, Missouri. The interview went fine, but when I came out of their office in the afternoon and turned on the car radio, I began to hear news bulletins about a place in Pennsylvania called "Three Mile Island". I figured it was a sign. :-)

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

Single-pipe failures

Kenneth Ng <KEN%ORION.BITNET@wiscvm.wisc.edu>
Wed, 29 Jul 87 06:26:11 EST

> [Concerning SINGLE-FAULT-TOLERANT SYSTEMS, I noted recently that most
> of the nuclear power plants are designed to remain safe as long as only
> a single pipe ruptures. Two pipes are too many. Earthquakes could make
> things quite difficult. PGN]

First, I'd like to point out that I am not an expert in nuclear energy or nuclear power. I am not entirely familiar with the workings of the insides of nuclear power plants. Even if I were, the fact that there is no standardization among these plants makes quantitative statements difficult.

Judging from "The President's Commission on The Accident at Three Mile Island", there are three methods of cooling the reactor:

1: Main feedwater pumps.
2: Auxiliary feedwater pumps.
3: High-pressure injection pumps.

Unfortunately among this foot-thick stack of reports I cannot find a blasted diagram of the reactor cooling system. I presume these systems operate on separate lines. But for all I know they could feed into a common line (besides the reactor vessel itself). Breaks in the upper half of the cooling system are covered however. Parts of the contingency plans indicate that it is possible to pump water that comes out of a break back into the reactor via sump pumps. Therefore, from what I can gather, two double-guillotine breaks that occur in the lower leg of the reactor cooling system may be fatal, but two double-guillotine breaks, where one occurs in the lower leg might not be fatal. Note: from the definition of double-guillotine breaks, isn't this four pipe breaks in 2 pipes?

Ref: double-guillotine break: a pipe break where a section of pipe is completely removed from the line (needing 2 breaks) and the outgoing water does not impede the flow of water coming out the other pipe. I read this somewhere in WASH-1400.

Hacking and Criminal Offenses (Re: RISKS 5.18) (David Sherman)

<ptsfa!pbhya!seg@Sun.COM>
Tue, 28 Jul 87 14:10:46 PDT

In reference to the above subject of Computer Crime, I have a book at home that told of a case of a stolen program for estimating bids on the type of work involved by two competing companies. The only reason the larger company was convicted for the theft of the program from it's smaller competitor was that they printed out a hard copy of the program. U.S. law at that time said that what was contained in electronic memory, wasn't "real?" or something to that effect. There certainly is a need for new or more comprehensive laws due to new technology. I also understand banks are required to make hard copies of their accounting programs determinations at appropriate places for auditing purposes. Again what is in memory is not "real".

SEG, Pac Bell, Rohnert Park, Calif.

Passwords and telephone numbers

<Jonathan_Thornburg%UBC.MAILNET@MIT-Multics.ARPA>
Tue, 28 Jul 87 20:51:42 PDT

This is an old pet peeve/idea/complaint of mine that some recent postings on passwords being broken have finally prompted me to set down on iron oxide:

Claim: Any frequent computer user, including the most non-technical, can/should be able to remember a 10 to 15 character password consisting of a "random" sequence of digits.

To demonstrate this, consider the following 2 questions:

(A) What's your office phone number?
(B) What's your home phone number?
I suspect almost everyone can answer both questions correctly. The two together give 14 fairly patternless digits, or 8 if you don't count exchanges.

Now compare the frequency with which you dial/speak/write your *own* phone number with the frequency with which you type your password. (This is why I only make my claim for any "frequent" user). At least around here, the number labels on office phones are often missing, so the lack of visual feedback for passwords shouldn't be a problem.

- Jonathan Thornburg userbkis@ubcmtsg.bitnet
thornburg%ubc@um.cc.umich.edu

Separation of duties and "2-man control"

"Patrick D. Farrell" <Farrell@DOCKMASTER.ARPA>
Tue, 28 Jul 87 15:32 EDT

Although Ted Lee's interpretation of "2-man control" does describe a form of implicit separation of responsibility, I suspect that Dr. Ware was referring to what has become rather common in NATO defense compusec procurements, the explicit "2-man (or more) rule". This a mechanism whereby two (or sometimes more) mutually cooperating, authorized administrators are required to perform some action that affects the state (particularly the security state) of the system.

The cooperating, authorized administrators may also be required to belong to separate operational groups, etc., depending upon how the system has been screwed together. All in all, it's not a bad idea and I'm still surprised that the US compusec community has not yet picked up on it.

Pat Farrell (Control Data Corporation)

Search RISKS using swish-e

THE RISKS DIGEST

Forum on Risks to the Public in Computers and Related Systems

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

Volume 5: Issue 20

Thursday, 30 July 1987

Contents

Lack of sanity at the IRS

"Victor S. Miller" <VICTOR%YKTVMZ.BITNET@wiscvm.wisc.edu>
30 Jul 1987 16:41:11-EDT (Thursday)

The following incident may seem familiar, but given the extreme dread and terror that many people find in the IRS, it could be quite serious:

My father-in-law is retired (and has been for a few years), but ocasionally works. My mother-in-law is still working. When she filled out their tax returns this year, she filled in the amount of social security payments received in the calendar year (as required), which was the maximum of $10,400 (I think). However, in transcribing the rough copy of the tax return to the final copy, she made a mistake and copied the vertical line between dollars and cents as a 1. Thus she filled in 104001.

About a month later they received a letter from the IRS stating that recomputation of their taxes showed that they owed another $4,500! Needless to say, they were quite upset until they realized what had happened. After it was pointed out, the IRS eventually cleared things up. It would seem that the simplest sort of sanity check in the figures would have eliminated

such behavior. The amount of social security benefits for a tax return with two dependents can't be anywhere in the neighborhood of $104,001. I wonder if there any sanity checks at all in the code?

Victor S. Miller -- IBM Research victor@ibm.com

[I thought you knew:
When it comes to the IRS, there is no Sanity Clause. PGN]

Hot Stuff [and Air-Cooled Gould?]

Burch Seymour <gould!augusta!bs@seismo.CSS.GOV>
Thu, 30 Jul 87 15:33:53 EDT

I spent a year working at Large Manufacturer of Space Craft. One of my duties was system manager of a large Gould Supermini-computer system. This was a dual processor ECL based system with 16 Megabytes of memory and about 2 Gigabytes of disk, plus lots of I/O controllers. One of the last things I did before leaving was start the paper work to get the system certified for classified operation.

Two years later.. I am talking to my former boss there and he says that the computer had been very unreliable lately. I am surprised as it was *extremely* reliable during the time I was there and ask what happened. It seems when the system went classified, they put locks on the doors -- which precluded normal security patrol checks. They also put the only audible temperature alarm in the room with the computer. One Friday night, the A/C went out. Monday morning (according to the report I got) the machine's cabinet was too hot to touch. This is not hard to believe as an 18 board ECL CPU puts out LOTS of heat, and this is a dual CPU system. Anyway ever since that incident, the machine has been flaky.

Gee, I wonder why? I'm amazed that it works at all. -Burch Seymour-

---

Re: Nuclear power plant monitoring and engineering

Brian Douglass <brian%asci.uucp@RELAY.CS.NET>
29 Jul 87 10:04:07 PDT (Wed)

This article is in regards to Leff's article in RISKS-5.17.

>If nuclear power plants were removed and replaced with coal burning plants,
>more people would die from the radiation released into the atmosphere by the
>burning coal. This ignores the death toll from coal mine accidents and air
>pollution. In short nuclear power plants are about as risk free as one can
>get in this society and our energies are much better off being devoted to
>automobile accidents, cigarrette smoking and alcohol addiction.

I've often heard these statistics and believe in their validity, as a statistic. However, what is not talked about is the potential death per accident. If a car crashes there is a reasonable chance somebody can survive (seat belts, luck), but that probably someone will die. In an airliner crash,

your chances of surviving are nearly nonexistent, with the body count surely in the hundreds. Although the chances of an accident in a nuclear plant are small, the potential body count is astronomical.

After Chernobyl, I heard an engineer say the odds of a nuclear accident was once in 10,000 years, but that the accumulated operating time of all reactors world wide was over 10,000 years! Does this mean we should expect a major accident about once every 30 or 40 years? Yes, nuclear plants are the safest overall, and offer better long term energy resources (look at France), but the chances of surviving the accident and potential body count of an accident must also be factored into the safety equation. I don't think you can say nuclear power is safer than say coal power when you compare the number of coal related deaths (mining, processing, burning) versus the potential death from a nuclear power station accident. It does mean we must be much more careful with this fire than we have with other fires we've harnessed before, but we should not walk away from it. That would be a greater burden for future generations then we have the right to inflict.

Brian Douglass, Applied Systems Consultants, Inc. (ASCI), P.O. Box 13301
Las Vegas, NV 89103, Office: (702) 733-6761, Home: (702) 871-8182
brian@asci.uucp
UUCP: {akgua,ihnp4,mirror,psivax,sdcrdcf}!otto!jimi!asci!brian

[Don't forget nuclear wastes in your calculations! PGN]

Re: Credit card risks (Michael Wagner, RISKS 5.15)

Ross Patterson <A024012%RUTVM1.BITNET@wiscvm.wisc.edu>
Thu, 30 Jul 87 14:25:02 EDT

Amos Shapir is quite correct. AT&T credit card numbers consist of your 10 digit telephone number, followed by 4 random digits. Indeed, this is the basis for one of their "features" - the ability to "phone home". One can dial one's own phone number, and when prompted to key in the credit card number (by an otherwise unidentified "bong"), simply type the last four digits. The call will be accepted and your wife/husband says "Hi!".

This risk Amos mentions, involved in someone knowing your name, is obviously that, given the AT&T card numbers, all but the last four digits can be derived by "letting your fingers do the walking".

As to the Internation Number, at least in the AT&T case it's just a two character prefix to your phone number and a one digit suffix. Hi tech, right?

Incidentally, US Sprint does it much better. I just received my FONCARD (pronounced with a long O, e.g. PhoneCard) from them. The card number is 14 digits, none of which relate to my phone number, account number, or even area code. In addition, the card is bright silver, highly reflective, and the imprint is *not* in a contrasting color - it's the same silver. I have trouble reading it from 12 inches away, and I doubt it's possible to read over someone's shoulder.

Ross Patterson, Rutgers University

Re Passwords and telephone numbers (RISKS 5.19)

Brian Randell <br%kelpie.newcastle.ac.uk@Cs.Ucl.AC.UK>
Thu, 30 Jul 87 16:20:54 BST

Jonathan Thornburg's comment ignores the point that people do not normally expect to change their telephone frequently, and that when the number does change, it takes quite a while to memorise it again.

Passwords

"Keith F. Lynch" <KFL@AI.AI.MIT.EDU>
Thu, 30 Jul 87 00:56:46 EDT

> From: Jonathan_Thornburg%UBC.MAILNET@MIT-Multics.ARPA

> (A) What's your office phone number?
> (B) What's your home phone number?
> I suspect almost everyone can answer both questions correctly. The
> two together give 14 fairly patternless digits, ...

But I have only one phone and one office, and neither number has changed for years. I have accounts on about ten computers, with a different password on each. Passwords sometimes change as often as monthly. However, the only ones I write down are those that I cannot set myself.

It isn't difficult to think of passwords that is easy to remember but hard to guess. Run two words together, or use the initials of some phrase, or misspell some word or name. Of course you should never have the same password on two machines.

Another password risk is terminal programs which offer to remember your password for you. These should come with strong warning messages.
...Keith

Search RISKS using swish-e

THE RISKS DIGEST

Forum on Risks to the Public in Computers and Related Systems

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

Volume 5: Issue 21

Saturday, 1 August 1987

Contents

Macaquepit Monkey Business on 747

Peter G. Neumann <Neumann@csl.sri.com>
Fri 31 Jul 87 13:01:04-PDT

A monkey slipped out of its cage aboard a China Airlines cargo plane [before landing] at Kennedy Airport, forced the crew from the cockpit, and played with the controls before it was nabbed. ``He wasn't making any demands -- he wasn't trying to take the plane back home,'' said John Schneider, an animal control officer from the Port Authority who netted the 15-pound macaque monkey after a 90-minute game of hide-and-seek through the 747 jet. (The monkey had crawled out of the cargo area and into the flight deck.) [UPI, in SF Chronicle, 31 July 1987]

Re: IRS Sanity Checks (RISKS-5.20)

<willis@rand-unix.ARPA>
Fri, 31 Jul 87 10:30:34 PDT

Re the IRS ADP procedures. Several years ago I participated with a committee that reviewed the IRS long range planning for ADP upgrades. So the group got to know something about general procedures, although not intimate software details.

In these comments, I'm only offering perspective. I am neither defending nor criticizing what the IRS or other record-keeping organizations do.

The IRS obviously runs an enormous financial operation. The accounts receivable is huge so that there is a high motivation to get tax payments processed and into the bank. Similarly the IRS is obligated under law to pay interest on delayed rebates, so there is a corresponding motivation to process tax returns rapidly. Both motivations are really in the citizen's best interest.

The first thing that happens to any personal tax return (at the regional processing center -- Fresno for California and the western states) is data entry directly from the submitted form and as written. The data entry clerks have no authority to change anything. The system then runs out the numbers according to the rules that go along with the tax forms and tax law. All the system does is check arithmetic, and probably verify the presence of required parameters (e.g., SSNs).

If it finds any variance, the computer generates an appropriate letter which is then mailed, sofar as I know without human review. A lot of people have been the subject of a completely automated action -- including a computer generated letter -- from detection of a problem to mailing of a letter.

At some point (I don't recall exactly when), all tax records are mag-taped to West Virginia to the IRS national processing center where they get additional checking, verification, examination, extraction of statistical data, etc. It's from this 2nd stage process that returns are selected for audit, and that produces the statistical parameters which go into the famous "computer evaluation" for audit selection.

The IRS motivation is to collect taxes accurately, according to law, and in timely fashion. While I don't know this from first hand evidence, I can imagine that there is little management motivation to include reasonableness checks on the taxpayer-submitted numbers and forms. Among other things, it could be a legal misstep to guess what the taxpayer intended to write, as opposed to what was actually written; and one can readily conceive circumstances under which the IRS -- or many other recordkeeping organizations -- could get into hot water by second guessing what a person intended to do on some form or in some transaction.

So, we're not likely to see many computer-based reasonableness checks in record-keeping systems, especially finanical ones. The error-correction feedback loop will continue to be external and through the individual concerned, as it has been for a long time with paper-based systems. Such a decision is partly legally based, partly because there is generally little basis for guessing what was intended, and partly because the operational costs will always act to minimize the amount of software that must execute to process each transaction.

While any computer-wise person can imagine all sorts of checks to improve the lot of individuals who have to deal with a records system, I'm afraid that managers of record-keeping activities are just not going to be motivated to implement subscriber-courteous safeguards.

PGN - your parenthetical comment about "There is no Sanity Clause" goes for many record-keeping organizations, not just Federal institutions.

Willis H. Ware, Santa Monica, CA

IRS Income

<Beckman@DOCKMASTER.ARPA>
Fri, 31 Jul 87 08:58 EDT

I am under the impression that the IRS is not supposed to release information they receive to other agencies. Hence, if someone says that there are receiving $104001 from SS, the IRS is apt to accept that, believing, perhaps, that these people are fraudently obtaining multiple checks to which they are not legally entitled, but report such income so as not to be in violation of the law under income-tax evasion sections. I am reminded of the story of the pest exterminator who put "Hired killer" under the occupation block.

Joseph

[The point of the message was that a reasonableness check on the SS field would certainly indicate that this return might deserve special attention -- without having to consult the SSA. PGN]

Re: Telephone access cards (RISKS-5.20)

<willis@rand-unix.ARPA>
Fri, 31 Jul 87 10:30:34 PDT

Re telephone cards, SPRINT, et al. Originally the GTE/SPRINT access code for making calls was just 7-digits for local calls, plus 2 additional ones when out of area. After getting the SPRINT switch via the local access number, the procedure was to dial the access code and then the desired number. The same thing was continued when it became US/SPRINT.

Penetrators of the SPRINT system have long been a problem, and all sorts of ways have been suggested for acquiring the access code. Among them was just plain automated PC-based exhaustive trials searching for a good one. At one time, my SPRINT business account got over 300 unauthorized calls in one month, ALL from Joliet, Illinois -- the location of a well-known prison. Given that I had always been extremely cautious about using the memorized number at a public phone, I never did find out how it got so popular in Illinois.

Recently, as noted in RISKS, the access code has become 14-digits but there has also been a procedural change. After getting the SPRINT switch

through the local access number, now the desired number is dialed first;
after a couple of beeps from the switch, the access code is then dialed.
It's a slight nuisance sometimes if one is using a phone that has the
buttons in the handset; he better get the receiver back to his ear fast or
the acknowledging beep-beep from the switch can be unheard.

One wonders why the inversion of parameters; here is a possible explanation
based solely on my conjecture, not on any first hand knowledge.

Given that penetrators will continue to be a problem, one would like to have
some data to help track them down or to have system characteristics that
will deter them. Clearly the 14-digit number makes guessing much more
tedious and possibly slow enough to turn away trouble makers. In addition,
if someone is trying to guess numbers, perhaps already knowing part of a
legitimate one, the system now knows what number is being sought when the bad
access code is given. As telephone companies have done for years, the called
party can then be contacted and asked who might be trying to make a call.

But the technique is at the same time so easily spoofed by calling any
number, or some public number (like an office building), or always calling
a different number each time while guessing at access codes. It's a minor
software extension to make the penetrator's PC generate a number to be
called in addition to generating a trial access code. Of course the
generated called number might not be a valid one which could mean that a
guessed access code would erroneously be discarded, but one can imagine
ways around such a small problem.

Perhaps there is no security connotation to the new SPRINT procedure;
perhaps it really stems from some software convenience, or some billing
requirement. Perhaps, also, the system designers bet on a security
safeguard that has little to offer. Perhaps the state-of-art for (what is
really) computer security in the telephone business is not as well advanced
as it is in mainframe world.

Willis H. Ware, Santa Monica, CA

Another comment on passwords (Re: RISKS DIGEST 5.19)

Robert Hartman <sun!rdh@seismo.CSS.GOV>
31 Jul 87 07:14:30 GMT

In response to Jonathan Thornburg's peeve/idea/complaint, it should be obvious
that any string of digits that can be attributed to an individual by a few
simple database lookups isn't a good candidate for a secure password. Your
random hacker might miss, but your diligent government could get right in.

Perhaps not the most reassuring thought. -bob.

[Like the "Yes, Virginia, there is a Santa Claus" letter that reappears
once a year in the European edition of the Herald Tribune, this
discussion keeps recurring in RISKS. I try to staunch it, but it seems
to take on a life of its own. PASSWORDS ARE INTRINSICALLY WEAK. THERE ARE
TOO MANY WAYS TO FIND COMPROMISES. Passwords might be considered better

than nothing, but only if people don't believe in them blindly -- in which case NOTHING might be even better, relying primarily on establishing communities of equal trustworthiness. At any rate, I have closed the spigot on several other messages on this subject that get into second- and third-order ramifications without confronting the deeper issues.

[While on the subject of spigots, we also received a flood of messages on nuclear power. They have been getting farther and farther from RISKS relevance, and thus are not included here. Jef Poskanzer [unisoft!jef@ucbvax.Berkeley.Edu ...ucbvax!unisoft!jef] suggests that the sci.misc USENET newsgroup is a more appropriate place for the not immediately RISKS related contributions. PGN]

Re: Origin of term "artificial intelligence"

Dave Benson <benson%cs1.wsu.edu@RELAY.CS.NET>
Thu, 30 Jul 87 14:36:22 PDT

Jon Jacky (<>):
<>... the term
<>"artificial intelligence" was originated in the 1950's by John McCarthy,
<>generally regarded as one of the most important computer scientists (he
<>invented LISP, among other things). The story goes that he created the term
<>in a grant application in order to kindle funders' interest in topics like
<>symbolic logic with otherwise seemed rather esoteric and impractical.

That's not the way John McCarthy tells the story. He indeed wanted to create

---

FDA opportunity for system safety person

Frank Houston <houston@nrl-csr.arpa>
Fri, 31 Jul 87 11:18:05 edt

FDA is seeking a person versed in system safety, especially computer system safety, to help advance the state of the art in medical systems. The job will involve both research and routine and requires a fair amount of experience in software. FDA would be willing to help train in the medical part.

Anyone interested should contact me at (301)443-5020 or mail a resume soon to my attention at Food and Drug Administration, Center for Devices and Radiological Health HFZ-142, 12720 Twinbrook Parkway, Rockville, MD 20857.

Frank Houston, Biomedical Engineer, Food and Drug Administration

---

Report problems with the web pages to the maintainer

Search RISKS using swish-e

THE RISKS DIGEST

Forum on Risks to the Public in Computers and Related Systems

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

Volume 5: Issue 22

Monday, 3 August 1987

Contents

Home of IBM computers succumbs to telephone computer up-down-upgrade

Peter G. Neumann <Neumann@csl.sri.com>
Mon 3 Aug 87 11:11:10-PDT

New York Telephone's Poughkeepsie-area central offices experienced a backfired attempt to upgrade the software for the (non-IBM) computers on 18 July 1987 in order to improve service for 50,000 customers in the area. The result was that for 21 hours only about one call in three got through for 8 exchanges, according to a NYT spokesman. Between 12,000 and 14,000 customers were reportedly affected. The problems were eventually solved, but the spokesman said the actual cause was still not known. [Source: Poughkeepsie Journal, 19 July 1987]

The article was contributed via US Mail by Ronald S. Rosen of Poughkeepsie, who noted that despite the public explanation of only one in three calls

making it through, there were some customers (Ron among them) who could not make ANY CALLS AT ALL. (Statistics are fine unless it is YOU to whom they refer.) PGN

Re: IRS Sanity Checks

Jerome H. Saltzer <Saltzer@ATHENA.MIT.EDU>
Sun, 2 Aug 87 23:40:58 EDT

> Subject: Re: IRS Sanity Checks (RISKS-5.20) [From RISKS-5.21]
> From: willis@rand-unix.ARPA
> Among other things, it could be a legal misstep to guess what the
> taxpayer intended to write, as opposed to what was actually written ...

It seems to me that second-guessing isn't the real RISKS issue here, but rather what should the program do if the reasonableness check returns the answer "unreasonable!"?

For the IRS case, with some hundred million returns per year to process, the simple answer of "kick it out for human review" could easily generate work for several million human reviewers. Where can you find that many reviewers all of whom are motivated to get to the bottom of the problem? One way to find an interested reviewer is to send the problem to the person who filed the return originally. Thus the IRS strategy of generating a completely automated kickout letter to the original filer is probably both more cost- and procedurally-effective than any alternative one could think of.

Admittedly, it is a little unnerving to receive an automated response from the IRS asking you to send them an extra $10,000,000.17 because the computer didn't realize that was a typo on line 11, but once you get over the initial shock, all you have to do (in principle) is follow the instructions for filing an amended return and the problem goes away. (Horror stories about IRS agents following up with inappropriate actions don't alter the appropriateness of this strategy; they instead illustrate a misfeature in a different part of the system.)

Jerry

[A missing reasonableness check bit me today. One of my multiple archive files for RISKS volume 5 had vanished: each issue had simply disappeared into a black hole. The file was totally invisible, but I noticed an unaccountable directory overflow. Creating a new version, TOPS-20 prompted with a NEW version number with protection "P1" instead of "P775252. Mark Lottor suggests that in recovering from a recent system crash no one had run the disk reasonableness check... PGN]

Re: Monkey business (clarification) (RISKS 5.21)

Peter G. Neumann <Neumann@csl.sri.com>
Mon 3 Aug 87 10:35:34-PDT

The item in RISKS-5.21 on the macacque-eyed 747 takeover was unfortunately

less than precise, possibly leaving the impression that the monkey comandeered the plane in flight. The monkey was at large in the cabin toward the end of the flight. After landing the pilot and copilot remained in the cockpit until the animal control officer thought he had the monkey cornered at the rear of the plane. After the pilot and copilot left, the monkey then entered the cockpit and was captured while sitting on the instrument panel between the pilot and copilot seats. [RISKS item: did the monkey alter any of the control settings? Presumably the next take-off checkout would have spotted it...]

Sorry if my attempt to be brief came off half-(ma)cacqued. PGN.

Computer (claustro)phobia

Kent Paul Dolan <kent@xanth.cs.odu.edu>
Sun, 2 Aug 87 13:51:29 EDT

Once upon a time, we had computers carefully confined in their own circumscribed environments, hidden away in air conditioned rooms, caged like the "extinct in the wild" species at zoos, and the earth was safe for humankind.

Now, I look around me: a Commodore Pet, an Apple II+, an Amiga 1000, and a Dimension 68000 occupy various horizontal surfaces. Floor to ceiling on two sides are shelves of 5.25" disks, 3.5" disks, back issues of Byte, collections of ACM and IEEE computer journals, manuals for the various systems, computer science textbooks, the collected works of ANSI X3H3 for 4.5 years, stray 1/2" mag tapes, old listings.

Have Forum readers considered the risk that, like the prairie by the pavement, we will simply be crowded out, displaced, inundated, overwhelmed, buried, by our high-tech toys?

Kent Paul Dolan

Security-induced RISK

Alan Wexelblat <wex@MCC.COM>
Mon, 3 Aug 87 11:49:25 CDT

At our site, we have several computers. For security reasons, we are asked to have different passwords on each machine. In addition, these machines (may - I'm not sure) keep logs of incorrect userid/password combinations that are entered.

Now, being a fallible human, I occasionally type the id/password for machine A while trying to log on to machine B.

It would not occur to me (in advance) that the log of incorrect combinations should be safeguarded, but imagine if that log fell into malicious hands. The attacker would have a list of excellent possibilities to try out on other machines at the site!

And, to make matters worse, while he was randomly trying combinations
from the log, he would be duplicating a "normal" pattern of errors,
thus being less likely to raise an alarm.

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

[This is a very old problem, and has been noted here in other connections before. Audit trails are littered (often quite accidentally) with sensitive information. Once again, the tip-of-the-iceberg phenomenon is seen. The deeper you dig in security problems, the more you realize that there are always some very serious vulnerabilities... PGN]

Another ATM story [Sufficiently different to warrant inclusion]

Jeffrey Mogul <mogul@decwrl.DEC.COM>
3 Aug 1987 1832-PDT (Monday)

A friend of mine tried to withdraw money from a Versateller (Bank of America; she's a BofA customer). After asking her to re-enter her PIN several times, it told her to give up. She knew the number was the right one (she uses it several times each week) so the next day she went to see a human employee of the bank. This person tried to tell her that she had probably forgotten or misentered her PIN, but had to back down when several people behind her in line said that they had the same problem.

My first thought was that the problem was with the cards, not the PINs. Although some automatic tellers (such as the one I normally use) imply that the card is readable (by welcoming you by name before asking for your PIN), apparently Versatellers do not. Still, I would expect them to complain about an unreadable card before asking for the PIN.

I doubt the problem was with a specific ATM; my friend was using the one in Palo Alto, but she lives in San Francisco and presumably most of the other affected customers did not use the Palo Alto machine.

I'm also assuming that the PIN is verified with the central system, not locally by the ATM, since there was some delay before the ATM complained about her PIN, during which time it let her specify the transaction she wanted.

Sounds like the BofA system had spontaneously forgotten (or garbled?) a bunch of PINs. This leads to some interesting speculations: does their system lose other information (balances, for example)? Has it been compromised? Is there a "disgruntled employee" at work? Do banks often forget PINs?

SDI is feasible

Walt Thode <thode@nprdc.arpa>
3 August 1987 1103-PDT (Monday)

(From the July 31 _Government Computer News_ (without permission))

SDI Software is Feasible, AFCEA Report Concludes

In a 200-page report to be released in Mid-August, The Armed Forces Communications and Electronics Association will conclude that development of the needed hardware and software for the Strategic Defense Initiative is difficult but attainable.

The study, begun in April 1986 for the Defense Department's Strategic Defense Initiative Organization, was carried out by a committee of civilian scientists from industry and research institutes. Five panels were set up, to examine processors, software, networks, communications, and man/machine interfaces, all under the heading of battle management systems and command, control, communications and intelligence systems.

Although the report has yet to be released, its conclusions have been aired in public by study participants. Describing the hardware requirements as "more firmly in hand than the software," the report says that building the system's architecture around hardware will mitigate software problems.

Stuart J. Yuill of RJO Enterprise Inc., Lantham, MD, chairman of the networks panel, said he was impressed by the high quality of the study teams. He also noted that conclusions of the study reflected the "nearly unanimous" view of the experts.

The task of developing the software needed for the SDI has been described as impossible by some observers, who say that a perfect defense shield is infeasible, partly because it is untestable. The AFCEA report instead suggests that developing effective software will be possible, even though the requirements are complex. Thus the system software needs the most attention, it says.

Publicized Risks

<mnetor!utzoo!henry@uunet.UU.NET>
Sun, 2 Aug 87 22:08:43 EDT

[This is not particularly computer relevant (and you may omit it if relevance is in with you today) -- except that the conclusion is worth noting. But, please don't respond to the items that are less than relevant. Yes, it's my fault -- I could have omitted Mark Day's precursor as well -- except that it had a useful comment on a STILL EARLIER message... Iterated Mumble. PGN]

> Car wrecks and cigarette smoking kill more people than nuclear plants, sure,
> but the way that they kill people is very different. Car accidents
> generally don't affect a zone of several miles' diameter, forcing evacuation
> and abandonment of homes... [Mark Day, RISKS-5.18]

There is also the question of voluntary vs involuntary risks. However, the comparisons here are basically apples-vs-oranges. A much fairer comparison

is to other risks that are involuntary, affect a zone of several miles' diameter, force evacuation and abandonment, etc. There are such, and they get far less attention than nuclear risks. One is driven to conclude that the perceived seriousness of risks has much more to do with the amount of publicity than with the magnitude of the problem.

Some examples:

- There is apparently at least one place in the US where a dam failure would probably kill a quarter of a million people. The probability of dam failure is known to be nonzero, and they are much less carefully guarded against terrorist attack than nuclear plants. Do you know whether there is one upstream of you?

- The Bhopal disaster probably (I don't have numbers handy) killed more people than all nuclear accidents to date, Chernobyl included. There was noise about it at the time, but it's largely forgotten now. Do you know whether there is a plant handling such chemicals within, say, ten kilometers of you? Do you care?

- The largest peacetime evacuation in history had nothing to do with nuclear reactors. Hundreds of thousands of people were evacuated from the center of Mississauga (which is essentially a suburb of Toronto) when tank cars loaded with chlorine derailed a few years ago. How many rail lines are there within ten kilometers of you? Do the railroads using them observe any restrictions on what cargos they carry on those lines? How frequent are derailments on those lines? (Usually the answers are "several", "no", and "much more common than you think".)

People who raise the issue of nuclear wastes should look into the arsenic content of stack-scrubber sludge from coal-burning plants. That stuff is produced in far greater quantities than nuclear wastes, for comparable power outputs, and arsenic has *no* halflife -- it is dangerous *forever*. Here we have another comparable, arguably rather worse, risk that is largely ignored in all the uproar about nuclear power. Why? Less publicity.

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

Search RISKS using swish-e

THE RISKS DIGEST

Forum on Risks to the Public in Computers and Related Systems

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

Volume 5: Issue 23

Tuesday, 4 August 1987

Contents

Article on "Computer (In)security"

Jim Horning <horning@src.DEC.COM>
Tue, 4 Aug 87 12:10:05 PDT

ABACUS: THE MAGAZINE FOR THE COMPUTER PROFESSIONAL
Vol. 4, no. 4, Summer 1987, pp. 7-25
"Computer (In)security: Infiltrating Open Systems"
Ian H. Witten (Department of Computer Science, University of Calgary)

ABSTRACT: Beware the worm, the virus, and the Trojan Horse. Despite advances in authentication and encryption methods, computer systems are just as vulnerable as ever.

MINI-REVIEW: This article is chock-full of the sort of information that RISKS contributions keep saying can't be overemphasized. It is written at a level that can be understood by almost anyone who ever had to log into a computer system, and possibly by a congressman or corporate vice-president. Witten stresses that trust is transitive: If I trust you as a source (especially for software), I have thereby placed trust in everyone you trusted.

SELECTED QUOTATIONS:

Shared computer systems today are astonishingly insecure. And users, on the whole, are blithely unaware of the weaknesses of the systems in which they place--or misplace--their trust. Taken literally, of course, to "trust" a computer system as such is meaningless, for machines are neither trustworthy nor untrustworthy; these are human qualities. In trusting a system one is effectively trusting all those who create and alter it--in other words, all who have access (whether licit or illicit). Security is a fundamentally HUMAN issue. ...

It is comforting, but highly misleading, to imagine that technical means of enforcing security have guaranteed that the systems we use are safe. ...

Many systems suffer a wide range of simple insecurities. These are, in the main, exacerbated in open systems where information and programs are shared among users--just the features that characterize pleasant and productive working environments. ...

Throughout this article the word BUG is meant to bring to mind a concealed snooping device as in espionage, or a microorganism-carrying disease as in biology, not an inadvertent programming error. ...

Not only should you avoid executing their programs; take the utmost care in ANY interaction with untrustworthy people--even in reading their electronic mail. ...

The simplest kind of Trojan horse turns a common program like a text editor into a security threat by implanting code in it that secretly reads or alters files in an unauthorized way. An editor normally has access to all the user's files (otherwise they couldn't be altered). In other words, the program runs with the user's own privileges. A Trojan horse in it can do anything the user could do, including reading, writing, or deleting files. ...

One good way of getting bugged code installed in the system is to write a popular utility command. ...

The thought of a compiler planting Trojan horses into the object code it produces raises the specter of bugs being inserted into a large number of programs, not just one. ...

The trick is to write a bug--a "virus"-- that spreads itself like an infection from program to program. The most devastating infections are those that do not affect their carriers--at least not immediately--but allow them to continue to live normally and in ignorance of their disease, innocently infecting others while going about their daily business. ...

The neat thing about this, from the point of view of whoever plants the bug, is that the infection can pass from programs written by one user to those written by another, gradually permeating the whole system. Once it has gained a foothold it can clean up the incriminating evidence that points to the originator, and continue to spread. Recall that whenever you execute a program written by another, you place yourself in that person's hands. For all you know, the program you use may harbor a Trojan horse, designed to do something bad to you (like activating a cookie monster). Let us suppose that, being aware of this, you are careful not to execute programs belonging to other users unless they were written by your closest and most trusted friends. Even though you hear of wonderful programs created by those outside your trusted circle, programs that could be very useful to you and save a great deal of time, you are strong-minded and deny yourself their use. But maybe your friends are not so circumspect. Perhaps Mary Friend has invoked a hacker's bugged program, and unknowingly caught the disease. Some of her own programs are infected. Fortunately, they may not be the ones you happen to use. But day by day, as your friend works, the infection spreads throughout all her programs. And then you use one of them. ...

If you use other people's programs, infection could reach you via a floppy disk. ...

The smaller and more primitive the system, the safer it is. For absolute security, don't use a computer at all--stick to paper and pencil! ...

The only effective defenses against infiltration are old-fashioned ones. ...

Finally, talented programmers reign supreme. The real power resides in their hands. If they can create programs that everyone wants to use, if their personal libraries of utilities are so comprehensive that others put them on their search paths, if they are selected to maintain critical software--to the extent that their talents are sought by others, they have absolute and devastating power over the system and all it contains. Cultivate a supportive, trusting atmosphere to ensure they are never tempted to wield it.

DC sends bad tax bill to the *WRONG* citizen

Joe Morris (jcmorris@mitre.arpa) <jcmorris@mitre.arpa>
Tue, 04 Aug 87 11:13:23 EDT

The District of Columbia, still smarting from its handling of the snow last winter, has discovered what happens when it sends out an erroneous tax bill to someone who can make life uncomfortable: it sent a bill for ten cents to David Brinkley (yes, THAT David Brinkley) along with a sternly worded warning that if he did not pay, he would be fined $2,137 in penalties and interest. Brinkley reported on this in a brief commentary on his nationally televised ABC news program last Sunday. There was a follow-up in this morning's Washington Post, from which the following is lifted:

> The whole thing was a mistake, said D.C. Department of Finance and Revenue spokeswoman Brendolyn McCarty, a "mathematical audit error." Ordinarily, she said, [taxpayers] would not have been billed for amounts of less than $2. But someone forgot to tell the government computer that.
> [...]
> Brinkley paid the 10 cents even though he maintained he owed the District government nothing. District officials acknowledge that his bill had been paid last year, but no one knows where the extra dime cropped up and officials cannot account for why the letter threatened him with $2,137 in penalties and interest.
>
> "They will wind up blaming it on the computer," Brinkley said when told of the District government's response. "I knew that. But a computer only puts out whatever you put in it."

Perhaps the most astounding thing to come out of this is that we apparently have at least one respected national news commentator who is aware that GIGO means "garbage in, garbage out", as opposed to most of the Fourth Estate, who believe that it means "garbage in, gospel out". The story itself, of course, is unusual only in its victim's ability to strike back quickly.

New Report on SDI Feasibility

Mark S. Day <MDAY@XX.LCS.MIT.EDU>
Tue 4 Aug 87 10:54:52-EDT

> Describing the [SDI] hardware requirements as "more firmly in hand
> than the software," the report says that building the system's
> architecture around hardware will mitigate software problems.

If this is an accurate summary of the report's conclusion, it's rather odd. The Eastport Study Group report to the Director of SDIO (December 1985) came to the exact opposite conclusion. Again, there was the assertion that the task of building SDI was "difficult but possible." However, there was also a strong critique of the usual procurement process of acquiring hardware first and treating software as an afterthought.

> ... contractors treated the battle management computing resources and software as a part of the system that could be easily and hastily added. The contractors treated battle management as something that is expected to represent less than five percent of the total cost of the system, and therefore could not significantly affect the system architecture. They have developed their proposed systems around the sensors and weapons and have paid only "lip service" to the structure of the software that must control and coordinate the entire system. (p. 9)
>
> The panel cautions, however, that the feasibility of the battle management software and the ability to test, simulate, and modify

the system are very sensitive to the choice of system architecture.
(p. 10)

It's plausible that the newspaper got it wrong and that the new report also says that designing the system around the SOFTWARE would make the software problem easier. Otherwise, it seems like a very strange claim.

Railway automation

Stephen Colwill <mcvax!praxis!steve@seismo.CSS.GOV>
Fri, 31 Jul 87 14:50:28 BST

This article follows up on previous comp.risks items relating to the Muni Metro and BART railway systems in San Francisco.

Today I was amused to read in The Times an article describing a ride that the Queen took on the new London Docklands Light Railway. This railway features driverless trains. The article describes an incident whereby overriding the control computer to "speed the royal passage" resulted in a delay occasioned by the doors not opening at the station because the train was improperly docked.

I was considerably less amused to read, as an aside in the same article, about an incident in which one of these automatic trains "crashed the terminus buffers and ended up dangling in midair". As I recall, the train was on the verge of leaving the end of some kind of bridge.

Although the Queen officially opened the LDLR yesterday passenger services would be delayed for a few weeks since (according to London Transport) "test running has not yet reached the high level of reliability needed".

I would like to express two personal opinions: firstly I am dismayed that despite the long history of railway travel each new implementor of automation still makes the same mistakes as the predecessors. Secondly I fail to see how people who propose automatic control of nuclear power stations and ATC can presume to do this when the conceptually far simpler problem of the control of trains on a closed railway network has not yet been solved after years of trying.

Steve Colwill, Praxis, Bath, England.

Any above-expressed opinions may not be imputed to my employer.

[Fault-tolerant imputers? PGN]

Faults in 911 system caused by software bug?

Jim Purtilo <purtilo@flubber.cs.umd.edu>
Tue, 4 Aug 87 11:00:53 EDT

I came across this the other day:

FAIRFAX'S 911 BACK ON TRACK
Shutdown Attributed To `Bug in Software'

Patricia Davis
The Washington Post, August 1, 1987

Fairfax County officials said yesterday that their new and occasionally dysfunctional 911 emergency communications center was operating properly, with calls being answered in less than a second.

Mike Fischel, director of the Public Safety Communications Center, said that American Telephone & Telegraph Co. workers had discovered and repaired a problem in the telephone system that a week earlier caused it to shut down for 30 minutes.

Because of a ``bug in the software,'' Fischel said, employes where able to receive calls at the communications center July 24 but could not hear the caller. Because of a backup system, however, there were no delays in providing emergency service, he said.

Although there have been ``persistent problems'' with the telephone system, including telephone sets overheating and some background noise, the computer-aided dispatch system has performed well since it became the primary system July 23, Fischel said.

The new system cost $12 million and is calld CAD, for Computer Aided Dispatch. It is housed in the police department's Pine Ridge facility in central Fairfax and somewhat resembles Mission Control at the Johnson Space Center in Houston. Red numbers flashed on a wall show how long calls go unanswered.
[....]
The new system displays the phone number and the address, then verifies the information, assigns a priority to the call and relays the information to the appropriate dispatcher --- police, fire or ambulance.

During the month-long transition to CAD, there were complaints of delays both in answering 911 calls and rerouting them to the proper dispatcher. Officials said those problems were because of the complexity of the system and the fact that employes were initially doing double duty by monitoring the old system to check the performance of the new one.
[....]
* * *

Hence it would appear that the new system failed but service continued due to the operators keeping both old and new systems on-line during a breakin period.

It would be interesting to find out a few more specifics concerning the nature of this ``bug.'' Does anyone out there have more clues to contribute? Also, once the glitch has been localized, it would then be interesting to learn ``who's responsible'' should the faulty system have resulted in some tragedy.

Jim

Re: Macaqueswain steering (RISKS DIGEST 5.21)

Peter G. Neumann <Neumann@csl.sri.com>
Tue 4 Aug 87 10:03:05-PDT

A query from Dave Mack wondered thoughtfully why on earth the monkey tale made it into RISKS. One reason is that I wanted to illustrate the point that developers of technologically based systems must anticipate all sorts of events that to the ordinary mortal would seem preposterous. Having a monkey loose in the cockpit is just one example of an event that few if any people had ever thought of before. I might have added something about monkeys typing randomly and sooner or later typing Shakespeare. The probability that a monkey might do something eventful to the plane controls is of course nonzero. Macaques are particularly inquisitive and playful. PGN [who is surprised that this prehensile tale has hung on in three consecutive issues!]

PIN-demonium

Curtis C. Galloway <cg13+@andrew.cmu.edu>
Tue, 4 Aug 87 13:33:30 edt

I used to think that bank card PINs were stored on the cards themselves, but an experience I had some months ago convinced me that (at least in my case) they aren't.

When I got my bank card from my bank in Little Rock, they didn't send me the usual notification of my new PIN. I assumed I could use the one I had requested on the application form, but it didn't work. I went in to my branch and they called up the central office -- they had assigned me a different PIN, but had never told me about it. The teller read off my card number to the person on the phone and they told her my number, which she wrote on the back of a deposit slip and gave to me.

Things were fine for a couple of months until one day an ATM rejected my card with an "incorrect PIN" message. I went back to the bank, where they went through the same procedure of calling the central branch. I found out they had changed my number back to the one I had originally requested!

I was very surprised at this -- I thought they had to give you a new card to change your PIN, or at least re-encode the magnetic stripe. Guess I was wrong...

--Curt Galloway
Internet: cg13+@andrew.cmu.edu
Usenet: seismo!andrew.cmu.edu!cg13+

Factory automation and risks to jobs

"James H. Coombs" <JAZBO%BROWNVM.BITNET@wiscvm.wisc.edu>
Tue, 04 Aug 87 13:18:02 EDT

The folklore has always been that computers, especially in the form of robots, would one day render blue collar workers obsolete. BIX [Byte Information Exchange] recently reported that automated assembly has not significantly reduced labor and assembly costs (and, presumably, jobs). Instead, inventory costs have been cut because planners can more accurately predict how long it will take to produce an item. Items can be produced "just in time" instead of maintained in inventory. In addition, resources devoted to assembly are only about 5 to 10 percent, but inventory tends to absorb 10 to 20 percent. The speculation now is that managers are more likely to be displaced than workers, since it is the managers who tend to be responsible for inventory management and accounting.

The BIX report [microbytes/items #1421] was based on the work of Randall Davis, a professor at the MIT Alfred P. Sloan School of Management and the MIT Artificial Intelligence Laboratory. Apparently Microbytes Daily interviewed Davis.

--Jim

Nukes vs Coal

Tom Athanasiou <toma@Sun.COM>
Tue, 4 Aug 87 10:26:54 PDT

> People who raise the issue of nuclear wastes should look into the arsenic
> content of stack-scrubber sludge from coal-burning plants. That stuff is
> produced in far greater quantities than nuclear wastes, for comparable
> power outputs, and arsenic has *no* half-life -- it is dangerous *forever*.
> Here we have another comparable, arguably rather worse, risk that is largely
> ignored in all the uproar about nuclear power. Why? Less publicity.
> Henry Spencer

I'm getting really sick of people defending nuclear power plants by talking about how dangerous coal power plants are. These are not the only alternatives, as we all should know by now.

As has been well established in the energy debates of the last 15 years, the best alternative to nuclear power is conservation. Please excuse me if I don't feel moved to dig the relevant factoids out of my library to back up this statement, as it should be obviously true. (You could, however, start with Lovin's classic SOFT ENERGY PATHS).

-- TomA

[OK, gang. Adequate discussion of the risks of technology in general may be impossible within the scope and resources of RISKS. Worse yet, there are deep belief systems involved, and some of the arguments are more religious than rational. I have had mail on both sides -- "Why do you keep running anti-nuclear power messages?", and "Why do you keep running pro-nuclear power messages?" I am just trying to keep RISKS objective, although very few people lack committed viewpoints in any argument -- the

rational middle-ground viewpoints do not seem to be popular in our society. (Moderation in the defense of moderation is no virtue?) One goal of RISKS is to encourage open discourse on topics relating to risks in computer-related technology. One perfectly good strategy in a particular area may be to eschew the use of computers in a particular application, or to avoid the application altogether. Such arguments may seem nontechnological, but they can be quite technologically based. PGN]

Search RISKS using swish-e

Report problems with the web pages to the maintainer

Search RISKS using swish-e

THE RISKS DIGEST

Forum on Risks to the Public in Computers and Related Systems

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

Volume 5: Issue 24

Thursday, 6 August 1987

Contents

Another animal story

Bill Pase <bill@ipsa.arpa>
Wed, 5 Aug 87 12:51:34 edt

I just got this out of the info-atari16 mail group.
It illustrates one of the more unusual risks I've seen :-)

> Date: 22 Jul 87 03:54:28 GMT
> From: mtune!akgua!rbk@RUTGERS.EDU (R. Brad Kummer)
> Subject: ST keyboard parts needed
> To: info-atari16@score.stanford.edu
>
> Does anyone have a damaged ST keyboard that they could send me a piece of?
> I need one of the little rubber "nipples" that sits under each key. If you
> remove all those tiny screws from the back of the keyboard, there is a

little rubber cup with a small piece of carbon attached underneath each key.

Why do I need it? Don't ask... My kids spilled a Coke on the keyboard, I took the keyboard apart to clean it (that part worked fine), but I dropped one of the little "nipples" on the floor and the [...] dog ate it!

If you could help me out, I'd be eternally grateful. (Would you consider trading it for a dog? :-)

Thanks, R. Brad Kummer, AT&T Bell Labs, Atlanta, GA {ihnp4, akgua}!akguc!rbk

[(Very lightly edited.) Doggone! PGN]

Re: Security-induced RISK

<mnetor!utzoo!henry@uunet.UU.NET>
Wed, 5 Aug 87 13:31:36 EDT

Those not in the Unix community may not be aware of the excellent security paper that was published in the Bell Labs Technical Journal a few years ago. Some parts of it are Unix-specific, but much of it is fairly generic. The most interesting parts are discussions of how supposed enhancements in security actually make things *worse*; the paper is clearly the result of practical experience, not just theoretical navel-contemplation. For example, the problem of logs of incorrect login/password combinations being a source of useful information is worse than it seems: even just logs of login names alone can be informative, because people do accidentally type passwords in response to the login-name prompt now and then. For another example, aging schemes that try to enforce frequent password changes have bad side effects: "...the most incredibly silly passwords tend to be found on systems equipped with password aging...".

The paper is "UNIX Operating System Security", by F.T. Grampp and R.H. Morris, AT&T Bell Laboratories Technical Journal, Vol. 63, No. 8, Oct. 1984, pages 1649-1672. Any good engineering library will probably have the B.L.T.J. (formerly the Bell System T.J.), since it is/was one of the top technical journals of the communications industry. This particular issue, the second special issue on Unix, can also be ordered from AT&T, although I don't have ordering details handy.

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

[While you are in that issue, you might just keep on reading. The paper following Grampp and Morris' is also worth looking at: "File Security and the UNIX Crypt Command", J.A. Reeds and P.J. Weinberger, pages 1673-83: "crypt" was not very secure. PGN]

Date: Wed, 5 Aug 1987 16:54 EDT
From: DAVIS%OZ.AI.MIT.EDU@XX.LCS.MIT.EDU

To: Risks@csl.sri.com
Subject: Factory automation and risks to jobs -- "apparently" not

From Risks 5.23: (Factory automation and risks to jobs -- James Coombs)
> The BIX report {on the effect of robots} was based on the work of Randall Davis, a professor at the MIT Alfred P. Sloan School of Management and the MIT Artificial Intelligence Laboratory. Apparently Microbytes Daily interviewed Davis.

"Apparently" is the key word here.

First of all, the information about robots and their potential impact on human employment is the work of Warren Seering (prof of mechanical engineering at MIT and a member of the AI Lab). An accessible (and quite entertaining) reference is his article in "Technology Review", April 1985 (pp 58-67); the impact and cost figures are on pp. 66-67.

All of which I would have been happy to tell BIX, had they asked. They didn't.

One of the RISKs of giving talks in public is having magazines quote as if from an interview (I don't recall an interview with BIX; I do use those figures as one slide in a 3-day long course). This curious procedure is apparently routine; it has in any case happened to me previously. The practice is at best disingenuous, suggesting that they have conducted a careful interview and summarized it, rather than picked a few entertaining sentences out of several hours of lecture.

It also quite often results in misinformation, as in this case. When you have an hour to explain a subject you do it one way; when faced with a reporter who is going to reduce everything to single sentence pithy quotes, you proceed quite differently (and quite a bit more carefully).

Railway automation

Scott E. Preece <preece%mycroft@gswd-vms.Gould.COM>
Wed, 5 Aug 87 09:06:09 CDT

> Stephen Colwill <mcvax!praxis!steve@seismo.CSS.GOV>:
> Secondly I fail to see how people who propose automatic control of
> nuclear power stations and ATC can presume to do this when the
> conceptually far simpler problem of the control of trains on a closed
> railway network has not yet been solved after years of trying.

I'm not sure I agree that controlling trains (actually operating them, as opposed to telling a human engine driver where she is supposed to go) is conceptually simpler than controlling a nuclear power station. A nuclear plant has a lot of sensors and actuators, in well known locations and required to be in well defined relationships to each other.

A train is a large object whose position is only approximately known at best, whose speed is hard to change and is changed using systems whose performance is subject to wild fluctuations with age, maintenance, and track conditions,

and whose surroundings are totally unvisible to the controlling system.

I wouldn't argue that a power plant is easier to control or safer,
but I think I would rate them similarly far beyond the realm of things I
feel comfortable about yielding to fully automatic control.

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

Nuclear generated electrical power and RISKS

Dave Benson <benson%cs1.wsu.edu@RELAY.CS.NET>
Wed, 5 Aug 87 13:32:19 PDT

Other fora ("forums" for those under forty) are perhaps suitable for
expressions of political position regarding the mix of electrical
generation methods, including conservation. We must recognize that
substantial computer related RISK is attached to nuclear reactor
generated electrical power, and that little computer related RISK
is attached to other generation methods or to conservation. I am
disappointed that so little commentary occurs in RISKS regarding
computers as realtime control devices of nuclear power plants.

My interest in seeing more such commentary should not be taken as a
political position regarding the appropriate mixture of electrical
generation methods. We might indeed all learn something about
mishap and accident prevention methods by learning more about what
is done in the nuclear power industry.

It seems perfectly consistent for a professional in computer related
areas to on the one hand be interested in learning more about computer
RISKS in nuclear power plants and on the other hand to take any
position whatsoever regarding the desirability of such.

I remind RISKS readers of the issues of AAAS Science, and the articles on
risks and risk perception therein, which I cited on RISKS a few months ago.

In conclusion, I hope we might continue to see in RISKS contributions
regarding computer risks in the nuclear power industry, without thereby
attributing to either our Dear Moderator or to the Contributor any particular
stance on the desirability of nuclear generated electrical power. I would
prefer the politics to appear elsewhere.

David B. Benson

[Me too. (By the way, now this issue of RISKS has both fora and fauna.) PGN]

PIN money?

<BJORNDKG%UREGINA1.bitnet@csl.sri.com>
6 Aug 87 14:11 CST

My credit union uses a PIN system that is designed in such a way that no one

is supposed to be able to obtain the PIN once it has been sent to you. The PIN is generated "randomly" and pre-sealed envelopes are produced with the PIN printed on the inside via carbon paper, and a serial number is printed on the outside of the envelope. When the PIN envelope is sent to a card holder, the serial number of the envelope is entered into the computer and the serial number is cross-referenced to the PIN which is then stored in that card's record. If you forget your PIN number, a new envelope with a new PIN is sent to you, because no one can access the actual PIN, only the computer knows what it is.

Of course, that is the theory, but I'm sure that someone somewhere can get to them given enough time.

[MILNET TAC access cards are generated the same way from a dedicated non-net-accessible system managed by the Network Information Center at SRI. PGN]

Re: Another ATM story

Scott Nelson <esunix!nelson@decwrl.dec.com>
Wed, 5 Aug 87 13:23:29 mdt

In RISKS 5.22: mogul@decwrl.DEC.COM (Jeffrey Mogul) says:
> A friend of mine tried to withdraw money from a Versateller (Bank of
> America; she's a BofA customer). After asking her to re-enter her PIN
> several times, it told her to give up...

This happened to me when I needed cash for the weekend (on a Saturday morning). From talking to the "ATM expert" at the credit union, I found out that the ATM asks you three times to re-enter your PIN, then determines that you should not be allowed any further transactions for the rest of the day. In my case it had a blank line where my name normally is when it first says "hello".

The solution, according to the ATM expert is to immediately hit cancel when the machine asks for your PIN a second time, clean the magnetic strip on the card, and try again. This method has worked since then. I don't understand why the ATM can't figure out that something is wrong when it reads the card. Don't they use checksums?

Assuming an ATM will work properly when you need it leads to the risk of being without any cash over a 3-day weekend. Now I only use them to avoid a long line inside during business hours.

Scott R. Nelson, Evans & Sutherland Computer Corporation

UUCP Address: {decvax,ucbvax,ihnp4,allegra}!decwrl!esunix!nelson
Alternates: {ihnp4,seismo}!utah-cs!utah-gr!uplherc!esunix!nelson
seismo!usna!esunix!nelson

``Computer `assumes' the worst in billing for hotel phone calls''

Bruce Forstall <forstall@larry.cs.washington.edu>
Thu, 6 Aug 87 09:25:59 PDT

Seattle Times, Wed. 8/5/87 (used without permission):

We knew it would happen eventually. Computers do this, computers do that. Now, we're told, computers *assume*. M.G., a Bellevue consumer, learned this when he tried to phone home from the Red Lion Inn at Portland's Lloyd Center. He phoned several times and no one answered, but he was charged for making long-distance calls. When he inquired about the charges, he was told the hotel computer ``assumed'' he had made a connection and talked with someone at the number he dialed. When M.G. explained to a live desk clerk at the hotel that no one had answered his phone calls, the charges were removed from his bill. M.G. suspects that many travelers pay such phone charges without realizing they've paid to hear a brrr-ring, not to speak with a real person.

Is this practice sanctioned by the Washington state Utilities and Transportation Commision? M.G. asked. Hotel and motel phone systems are private telecommunications systems, and are specifically exempt from regulation by state law, according to Susan E. Sumner, public-information officer for the commision. Sumner checked with Red Lion headquarters and was told the hotel's computer equipment cannot determine whether a call that has been placed actually has been answered. ``Consequently, in the first 45 seconds after a call has been placed, the computer `assumes' the call has been answered,'' Sumner said.

The hotel's policy is to adjust the bills of guests who have been charged for calls that were not completed. Red Lion's management has indicated that printed notices will be placed by phones in rooms so guests will know how they are being charged for these calls. It would be wise for consumers to ask about this policy when checking into any hotel. Some hotels and motels charge an access fee even when consumers use their own credit cards to make long-distance calls.

Shelby Gilje, Times staff columnist

--Bruce Forstall ...!uw-beaver!uw-larry!forstall

[Old-time RISKS readers who are still with us after two years may remember earlier discussions of this problem, or by now might have forgotten... PGN]

Search RISKS using swish-e

THE RISKS DIGEST

Forum on Risks to the Public in Computers and Related Systems

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

Volume 5: Issue 25

Sunday, 9 August 1987

Contents

Computer Error Opened Flood Gates of Alta Dam (Norway)

Haavard Hegna <hegna%vax.nr.uninett@NTA-VAX.ARPA>
Fri, 7 Aug 87 16:33:28 +0200

This excerpt (slightly edited) is from Dagbladet, Oslo, Norway,

Friday August 7. 1987:

COMPUTER ERROR OPENED ALTA (power station) FLOOD GATES. While all (Norwegian) electrical power supply directors were on visit at the very controversial and newly opened Alta Power Station (in Finnmark, northern Norway), the catastrophy happened. While trying to correct a computer error, two of the flood gates of the Alta Dam accidentally opened.

A three-meter high flood wave ran down the narrow river canyon at a speed of approx. 20 km/h. A full police rescue alarm was called, local radios gave warnings to campers etc., a helicopter was sent out to locate possible victims of the flood. The river rose about 1 meter during the twenty minutes that went by before the the dam engineers were able to close the gates manually. 2 million cubic meters (50 M cubic feet ?) of water was lost.

As far as the local police knows, no one was hurt, but 5-10 small river boats were crushed. The power station expects some claims for compensation. [The Alta river is well known for its salmon]

The Alta Power Station has been operative since May this year. "The paradox is that this very autumn we were going to install a valve that will prohibit the accidental opening of the flood gates", the dam administration says.

The Alta Dam and Power Station was much in the news a few years ago. It lies in the Norwegian part of Lappland. Long and very violent demonstrations by Lapps and others (including some very prominent Norwegians) nearly stopped the contruction work.

Haavard Hegna, Norwegian Computing Center, Oslo, Norway

Heating up planning discussions ...

<Robert_Slade%UBC.MAILNET@umix.cc.umich.edu>
Fri, 7 Aug 87 06:27:04 PDT

Regarding Burch Seymour's note in 5.20 about a CPU overheating: a certain charitable recently purchased computer equipment to assist with their operations. Bad planning contributed largely to the fact that it has not been of any help to them. One of the concerns that they failed to address was the physical placement of the machines with respect to heat.

A "Baby 36", a PC, terminals and printers for both and a printer for the new phone system were all put into an eight-by-ten-foot room. As the contractor hired to perform the initial installation of software, and training for the staff, I pointed out that this was less than desirable. However, it was not until, in an attempt to make the room habitable, I turned the thermostat off that I found out that it controlled not merely that room, but the entire back half of the building.

With the assistance of the materials manager (after failing to convince the executive director to make changes in room assignments) I completely blocked the heating duct into the computer room, and made a direct fan vent

to the outside. In spite of this, through one of the coldest winters we've ever had in Vancouver the temperature *never* fell below seventy-two degrees farenheit (most often it hovered in the eighties) and the clerical staff froze their fingers off.

(After three months of complaints of heatstroke and frostbite [one typist took to wearing gloves all day!] the computer was moved ... to an area with insufficient power supply!)

Re: Faults in 911 system caused by software bug?

<pgarnet@nswc-wo.ARPA>
Fri, 7 Aug 87 14:52:23 edt

Instead of being critical of the bug and the 30 minutes of downtime

>... it would then be interesting to learn 'who's responsible' should
>the faulty system have resulted in some tragedy.

we should find it refreshing to see that someone has learned the lesson of keeping the old system on line while the new one is tested *IN THE REAL WORLD*. So many times people disconnect the old system and depend entirely on a new, incompletely tested system.

Paul Garnett

"It must work, the contract says so"

<mnetor!utzoo!henry@uunet.UU.NET>
Fri, 7 Aug 87 17:20:51 EDT

Mark Day's comments re the Eastport report bring to mind a related issue, which has some relevance to Risks: how management responds to reports of problems. I highly recommend "Illusions of Choice", by Robert F. Coulam, published (I think) by Princeton U. Press, dated late 70s (I can dig out accurate info if needed; my copy isn't handy). The ostensible subject of the book is the development and procurement of the infamous F-111 fighter- bomber, but it is also a fascinating look at bureaucratic management and the mistakes it makes.

The title of the book comes from the persistent belief of the senior DoD people that they could decide the project's fate at various milestones during development, when in fact the project was merrily proceeding on its pre-ordained path without waiting for permission to do so. This was not because the people in question lacked authority: the F-111 had so much trouble that the Secretary of Defense was personally involved.

The part of the book that specifically came to mind was Coulam's comments on the F-111's engine problems: DoD repeatedly took it for granted that the engine problems would be solved, simply because the contract with the engine manufacturer said so. The engine problems *were* eventually pretty much solved, but only at the cost of significant changes to air intakes and so forth. Those changes were incorporated only in later F-111's, because

the early ones were too far down the production line by then: aircraft production had happily continued, in sublime confidence that the engine problems would go away!

This sounds a whole lot like the contractor attitudes that the Eastport group criticized. I would conjecture that the software development was going to be done by someone other than the prime contractor for the hardware. Of course the software would work on the hardware as supplied; the software contracts would insist on that!

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

---

Separation of Duty and Computer Systems (re: Pat Farrell, RISKS-5.19)

Howard Israel <HIsrael@DOCKMASTER.ARPA>
Sat, 8 Aug 87 18:00 EDT

Just as a point of fact, the COMPUSEC community has picked up on this. Any VAX/VMS system since V4.0 (I believe, V4.3 definitly) has the capability to enforce 2 passwords on a given account. This allows the system administrator to set up privileged accounts (or semi-privileged accounts, or just regular accounts) with 2 passwords, one user for each of these passwords. The capability to activate the account would require both users to be present to login. Once logged in, the user can do what he wishes (exactly analogous to the safe deposit box situation in a bank). Even the system administrator's account can be set up this way.

Of course, one does not have to necessarily use two people, just one person who knows both passwords would get you in also (I guess this is appropriate for especially paranoid people).

---Howard Israel, ATT Bell Labs

Southern Methodist University <Leff>
Fri, 7 Aug 1987 01:54 CST

<E1AR0002%smuvm1.bitnet@RELAY.CS.NET>
Subject: Optical Disks Raising Old Legal Issue
To: RISKS%CSL.SRI.COM@RELAY.CS.NET, INFO-LAW@BRL.ARPA

Summary of "Optical Disks Raising Old Legal Issue", in Digital News, 3 Aug 1987

When microfilm came out, Congress passed the Uniform Paperwork Act which covers "microfilm, microfiche, photocopies and some electronically transmitted paperowrk, such as facsimiles." There is a book out called the "Legality of Optical Storage" which was prepared with the assistance of a law firm. No specific state or federal laws cover the technology as yet. Robert S. Williams, president of Cohasset Associates in Chicago, a record management consulting form, says that the existing laws will suffice. New Jersey has a

bill pending in the legislature to specifically cover optical storage. It is geared to the state government's needs rather than private industry.

The IRS has already introduced a trial program in which optical disk juke box storage is used by personnel to answer questions from customers or in preparation for audit. However, the IRS still keeps the original forms although both the IRS legal counsel and Department of Justice says that the optically stored originals are as good as the originals in court. The National Archives has given IRS the permission to destroy the originals, but the IRS is still storing the originals.

AAAS Colloquium Notice

Stan Rifkin <rifkin@brillig.umd.edu>
Fri, 7 Aug 87 12:29:41 EST

The American Association for the Advancement of Science (AAAS) is holding its Second Annual Colloquium on Science, Arms Control, and National
Security September 28-29 at the Hyatt Regency Crystal City, jut outside of Washington DC. The reason Risks Forum readers should be interested is that this Colloquium represents one of the few occasions when policy-makers meet scientists to share concerns; both sides speak frankly.
For example, at last year's Colloquium, Kenneth Edelman, Director of the US Agency for Arms Control and Disarmament, said that nuclear weapons were safer now than at any other time in history. The Colloquium provided the opportunity to ask him what made him believe that. Last year Gen. Abrahamson, Director of SDIO, made clear that the first step in SDI was to protect military targets, not civilian populations. He also provided a list of technologies that needed to be developed in order for SDI to succeed. High among those was battle management software. He said that computing power alone can tip the strategic balance between the super-powers.

Speakers at this year's Colloquium will include Robert Dean, Special Assistant to the President and Senior Director for International Programs and Technology Affairs; Lewis Branscomb, Director of the Science, Technology, and Public Policy Program at Harvard, and formerly the Chief Scientist of IBM; Robert Cliff Duncan, Director of DARPA; John Deutch, Provost of MIT; Paul Nitzer, Special Advisor to the President and Secretary of State for Arms Control Matters; Jonathan Dean, Arms Control Advisor, Union of Concerned Scientists; Amoretta Hoeber, Director for Planning and Development, TRW; Lt. Gen. John Wall, Commander, US Army Strategic Defense Command; Charles Zraket, President, Mitre; and Sidney Graybeal, VP of Systems Planning Corp. Registration is $160 (incl. meals) for the two days. For further information, call AAAS at (202) 326-6490.

- Stan Rifkin

Secrecy About Risks of Secrecy Vulnerabilities and Attacks?

Peter J. Denning <pjd@riacs.edu>
Fri, 7 Aug 87 13:08:34 pdt

A recent item in RISKS called attention to Ian Witten's article in the summer 1987 issue of ABACUS. I found the article fascinating reading and filled with insight. It is crammed with detail on the weakness of systems to password attacks, Trojan horse attacks, and virus attacks, and it even elucidates the lacunae of Ken Thompson's Turing Lecture on invisible, self-replicating compiler viruses.

I would like to invite a discussion in RISKS on the question of publishing graphic detail on security weaknesses of systems. As Editor-in-Chief of the ACM Communications, I am sometimes faced with conflicting reviews on such materials -- some reviewers will say it is inappropriate to publish such lucid detail when there is no good defense against the attacks, some will say that this type of information is capable of inspiring a lot of mischief and making life unpleasant for numerous innocent people, while others will say that these things need to be discussed so that people of good will will know what they're up against. It would be helpful to me and other editors to have a better idea of where the community stands on this sort of thing. Should we encourage publication of this kind of material? Discourage it? Publish general overviews of attacks and weaknesses but not give enough detail to permit others to replicate the attacks? Should there be an ACM policy on this question? If so, what might that policy be?

Many thanks to all. Peter Denning

> [This topic has arisen regularly in RISKS. The last time we took a crack at it we still seemed to believe that vulnerability lists were somewhat sensitive, but the pretense that nobody knew what they might contain was likely to get you into much greater trouble than if you assumed that the vulnerabilities were widely known and likely to be exploited. If a system is fundamentally flawed, it should not be used in critical applications where those flaws could result in serious compromise. Publishing the security weaknesses can only improve things in the long run -- although it may lead to some frantic moments in the short run. The real problem is the tendency to put all of one's eggs in a single ostrich basket -- and then stick your head in the sand. Passwords are a fine example. If there is ONLY ONE PROTECTION WALL, then anyone who penetrates it has everything. The obvious strategy is to use multiple controls -- with passwords (or perhaps better authenticators) as a first line of defense, sound oerating systems and applications as a second, and careful auditing in real-time or after-the-fact as the last resort... PGN]

Another electronic mail risk

Doug Mosher <SPGDCM%cmsa.Berkeley.EDU@Berkeley.EDU>
07 Aug 87 17:55:16 PDT

I want to point out a hazard in electronic mail systems that can easily be overlooked until one gets caught by it.

The risks normally discussed include: the mail gets seen by unauthorized readers; is lost; is sent but the archive copy is later lost; the ID or contents are changed; or the recent and humorous example of "archive saved after all" when it wasn't wanted, in Reagan's NSA using PROFS.

The additional hazard I want to point out is: the problem of yourself inadvertently sending a note or a copy to the wrong person(s).

I have used various forms of e-mail at several universities over a 13 year period, and perhaps the most embarrassing incidents in such use have been when I mis-sent notes.

Typical sensitive contents are things relating to criticism, of employees or peers or managers. Or possibly semi-secrets, usually related to early discussions of hirings, firings, reorganizations, office moves, management shifts. All of these matters can be written about to specific individuals, where the mis-sending of the note can be very hurtful; in some cases if mis-sent to specific persons, in other cases if mis-sent to almost anyone.

Here's a brief list of ways such mis-sending can occur:

1. similar names or nicknames or userid's.

2. absentmindedness, along with interruptions; returning from a telephone interruption and sending a note to the proper recipients of the previous topic or the next topic.

3. the manual or automatic inclusion of others on a cc list for something to which you are replying.

4. mistakes or misunderstandings or similar names/nicknames/userids in group or system nickname files.

5. Actual failure of an electronic mail system (I have found this rarer than the above risks, though when I was developing some of my own tools once, I had this type of failure; the form of it was to mail the current note to the recipients of the last note I sent).

Electronic mail is riskier in this regard than manual mail, for several reasons, including:

Brief, cryptic, and/or indirectly indexed names for addressees; unusually fast and simple actions to prepare and send the notes, which avoid the normal delays with real mail (but those delays added extra chances for review by oneself and others, or chances to intercept and cancel); plus the normal risks of new or unfamiliar systems and the risks of computerized systems.

One defense is a broad defense against the dangers of many new systems: use the new facility for the least critical matters in the early stages of either the system's development or your learning of the system.

Doug Mosher, MVS/Tandem Systems Manager (415)642-5823,
Evans 257, Univ. of California, Berkeley, CA 94720

[Ironically, one solution here is related to a solution to Peter Denning's query: assume that everything might as well be public anyway (since the privacy and integrity in most mail systems and the networks they use are minimal anyway) -- and don't use a computer system to say anything that you would not say publically.

There are also some "features" of mail systems under which the current pointer does not get moved as you might think it would. You can easily wind up answering the wrong message. The solution there is always to review a message -- including its recipients' addresses -- before you commit to sending it off. PGN]

Risks TO computer users (US Sprint)

"James H. Coombs" <JAZBO%BROWNVM.BITNET@wiscvm.wisc.edu>
Sat, 08 Aug 87 15:32:16 EDT

Well, in addition to the risks to the innocent public from the use and misuse of computers, I now see that we computer users suffer because of the ignorance of those who apparently do not use computers or, at least, those who use them mindlessly. US Sprint has just dumped two different kinds of cards on me, neither of which works with my software.

I have Sprint's local basic service, but the quality is not good enough for telecommunications. Their "dial a local number and input a code" connection has always been better than AT&T or anything else that I have had locally. Now, however, they have numbers that are too long for ProComm. In addition, they have reversed the sequence, so that one now inputs the telephone number before the travel code. That means that none of the popular communications software will work properly with Sprint's new system. Finally, to demonstrate their complete ignorance of the needs of telecommunicators, they ask us to "listen for the recording" before inputing the "14 digit FONCARD number." It will probably take the ProComm authors a little while to come out with a speech recognition module!

This change is going to cost Sprint a lot of revenue in the next few months. It's also going to cost many of us a lot of aggravation. The software developers will have to rework their programs and negotiate with Sprint (or we will find different carriers). And, at least in the meantime, there will probably be a lot of people hacking together interim solutions. How could Sprint be so naive?

--Jim

P.S. If they are trying to solve problems with illegal access, they are on the wrong track. The thieves will revise their programs very quickly; the legitimate customers will be the ones who are locked out.

Computer Safety and System Safety (Re: RISKS 5.22)

<SAC.96BMW-SE@E.ISI.EDU>
9 Aug 1987 10:57-CDT

REF. YOUR CONTRIBUTORS WHO TALK ABOUT THE "SAFETY" OF THE COMPUTER. AS ONE WHO WORKS IN THE "SAFETY" CAREER FIELD I REALIZE THAT THERE ARE MANY FORMS OF "SAFETY", AND THERE IS A DEFINITE NEED TO MAKE COMPUTERS "SAFE" FOR USE. I FIND HOWEVER THAT IN READING THE PAGES OVER THE PAST YEAR AND A HALF THAT MANY OF YOUR CONTRIBUTORS ARE CONFUSING "SAFETY" FOR "SECURITY" AND SHOULD INSTEAD BE TALKING ABOUT COMPUTER SYSTEM SECURITY RATHER THAN COMPUTER SYSTEM SAFETY. (THERE IS AN ENTIRE SUB-GROUP OF THE SAFETY FIELD THAT DEALS STRICTLY WITH SYSTEMS SAFETY.)

AL WATTERS, SAC - Safety, Always Caring

Computers in nuclear power plants

Frederick Wamsley <well!alcmist@cogsci.berkeley.edu>
Sat, 8 Aug 87 23:20:11 pdt

Much has been said about the risks of trusting computers too much. It can also be a problem to trust them too little. This was a problem at Three Mile Island, where the human operators turned off a cooling system that the automation had turned on.

Good user interfaces can help. It should be clear to a human supervising an automated system *why* it's doing whatever it's doing. Observers on the presidential convention which investigated TMI said nasty things about the design of the plant's control panel.

By the way, anyone interested in the political aspects of nuclear power should check out Peter Beckman's book, "The Health Hazards of Not Going Nuclear".

Autoteller problems (Re: RISKS 5.22)

Alex Colvin <mac@uvacs.CS.VIRGINIA.EDU>
7 Aug 87 18:21:54 GMT

I've had a problem with my PIN on an autoteller before. In this case it was clear that the problem lay in the PIN keypad. Some keys wouldn't register, others bounced. After several attempts at typing very carefully, the machine kept my card.

Customer Service had noticed an unusual number of cards taken over the weekend, but were dubious of my explanation until several people in the customer service line behind me made the same complaint. They had me talk to the service people, because I was able to explain the problem in technical terms ("keys", "bounce").

It's possible the BofA problem was also a simple mechanical failure, but bank staff tend to treat the machines with reverence not accorded ordinary

household appliances. They don't expect them to get stuck and break.

[Several other ATM submissions are not included here. This one is borderline, illustrating again the deification of technology. PGN]

Search RISKS using swish-e

THE RISKS DIGEST

Forum on Risks to the Public in Computers and Related Systems

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

Volume 5: Issue 26

Monday, 10 August 1987

Contents

Secrecy About Risks of Secrecy (RISKS 5.25)

Jerome H. Saltzer <Saltzer@ATHENA.MIT.EDU>
Mon, 10 Aug 87 15:42:01 EDT

The desirability of public discussion of computer security flaws comes up frequently in RISKS as well as in every mailing list and forum I've seen that touches on security. My opinion is very strongly in favor of openness and public discussion of computer security problems, right down to the details of how to break in to specific operating system releases.

The background for my strong opinion is that I've been working with computer security, protection, and privacy since 1961. In that time I've seen both secrecy and openness used at different times, and it is clear (to me) that whatever arguments seem to apply at the time, in practice openness works and secrecy doesn't. Whenever someone succeeds in arguing that a security problem shouldn't be noised about, the result is usually several of the following:

1. Fixing of the specific problem drops in priority, sometimes to the point that it doesn't get fixed at all, leaving the

system vulnerable to attack for an extended time.

2. Others with similar systems often don't learn about the problem, leaving their systems vulnerable.

3. Others with dissimilar systems almost never hear about the problem and therefore don't realize that they should look for analogous problems in their systems.

4. People developing new systems design the same problem into their new system.

In contrast, when rapid public discussion takes place following discovery of a security problem, the original system gets fixed very quickly (sometimes it is temporarily operated in a drastically curtailed mode while waiting for the fix); other users of similar systems start evaluating their vulnerability, the community immediately starts to look for analogs of the problem, and as a general rule the state of the art steps forward a notch and that class of problem has a somewhat lower chance of reappearing in future system designs. (That is not to say that all system designers bother to look around for lessons they might apply to their systems!)

My conclusion is: the argument that one enhances security by not talking about weaknesses is fallacious. In practice, trying to hide security problems reduces security, certainly in the long run, usually in the medium run, and often even in the short run.

When the proprietor of a site or an operating system vendor makes a potent case for not revealing a security weakness, my usual proposal in response is that any veiling of a weakness should have a time limit, after which it will be discussed publicly. That approach focuses the argument on the right question, namely what is a reasonable time limit; it keeps the pressure up to fix the problem, and it tends to move in the direction of getting the information out to those people in the world who really need it. Most important, it recognizes that the information will eventually circulate among system attackers, so it must be gotten to system designers, too.

To say more strongly what Grampp and Morris wrote in 1984: the bad guys know this stuff already, or will discover it soon; the good guys need all the help they can get.

Jerry

[As an example, we have the note from BJORNDKG in RISKS-5.24 that "If you forget your PIN number, a new envelope with a new PIN is sent to you, because no one can access the actual PIN, only the computer knows what it is." But anyone who reads RISKS should realize how untrue this conclusion is, even if the PIN is stored encrypted! PGN]

Secrecy About Risks of Secrecy Vulnerabilities and Attacks?

"Maj. Doug Hardie" <Hardie@DOCKMASTER.ARPA>
Mon, 10 Aug 87 09:41 EDT

> Should we encourage publication of this kind of material? Discourage it?
> Publish general overviews of attacks and weaknesses but not give enough
> detail to permit others to replicate the attacks?

I am not convinced that you can publish overviews that do not provide any thoughtful person with enough insight to fairly easily complete the details of the attack. I believe that it is the initial identification of a flaw that is difficult, not the exploitation of it.

> [... If a system is fundamentally flawed, it should not be used
> in critical applications where those flaws could result in serious
> compromise... PGN]

While this argument appears logical from the academic view, it has some interesting ramifications in real life. Since the introduction of digital computers, the federal government has been one of the biggest users. Their usefulness has led to all sorts of sensitive information being stored and manipulated in an amazing variety of different machines. I believe it is fair to state that these machines were not designed with security as a major consideration. I suspect that removing all sensitive information from critical applications would cripple the government. Also, there is no way to replace all those systems with secure systems in the near future. Even if we only buy secure systems for new applications, it will be several decades before the fundamentally flawed systems are gone.

> [... Publishing the security weaknesses can only improve things
> in the long run -- although it may lead to some frantic moments in the
> short run... PGN]

Unless those frantic moments include the USSR concluding from compromised information that they are able to successfully attack the US. In that case, I claim that regardless of the outcome of the attack, publishing the security weakness did not improve things in any sense. -- Doug

---

Re: Separation of Duty and Computer Systems (RISKS-5.25)

<willis@rand-unix.ARPA>
Mon, 10 Aug 87 10:17:38 PDT

Just a clarifying comment on Howard Israel's observation about VMX/VMS. It may be that the tekkies have provided for the option of twin passwords but government policy statements and administative directives have not directed that such safeguard procedures be used. Until system implementers and system owners/operators are compelled to install split-duty provisions, the best intentions of the technical designers will only have provided a necessary, but not sufficient condition for improving security. We will have happenstance usage of double passwords depending on the conscience of system managers and their perception of threat.

And in some sense, as Howard Israel points out, the safeguard as now implemented isn't all that great since one person, knowing both, can type them in sequentially -- which makes it no better than a single password and certainly more trying to one's memory. A stronger procedure would require concurrent entry (within a prescribed time limit) and from different, physically well-separated terminals. Even that can be circumvented as Richard Pryor once demonstrated in some movie.

The importance of such intricate safeguards of course depends markedly on what the threat is believed to be, which implies that double passwords will probably be used primarily in defense systems and occasionally in commercial systems, e.g., perhaps where public safety or intense industrial competition might be involved.

Willis Ware, Santa Monica, CA

NASA Computers Not All Wet

Mike McLaughlin <mikemcl@nrl-csr.arpa>
Mon, 10 Aug 87 08:44:57 edt

A recent news items noted the flooding of a NASA control room during a simulated Space Shuttle flight. A longer piece on NPR stated that pipes in the ceiling of the control room had burst, and that the control room crew had quickly put covers over their equipment. NASA personnel considered it "routine" to have equipment covers handy for just such an occasion. While it is easy to second-guess the installers, the NASA computer folks should be complimented for having their covers ready. This is a simple, non-technical precaution. I'm surprised that it has not already been discussed in Risks.

> [It has, but way back in RISKS-1 or -2. By the way, there was a CDC computer in a basement that got flooded by the automatic sprinklers, shortly after I arrived at SRI. By the by-the-way, I heard a story today about a corporate building power failure that was accompanied by a fire; it turns out that the obligatory "EXIT" sign came on in the dark with a short in its circuitry, and the emergency light caught fire. (The bearer of this news wanted to keep his company's good name out of RISKS, so this is appears here anonymously.) PGN]

[Can't cite my sources - I was lazy, hoping someone else would enter a comment about this one, and I have forgotten the exact details, such as which center, what date, etc. - Mike]

Computer Error Opened Flood Gates of Alta Dam

<mnetor!utzoo!henry@uunet.UU.NET>
Mon, 10 Aug 87 14:14:58 EDT

Dept. of amusing juxtapositions: in 5.24 we have Dave Benson saying "We must recognize that... little computer related RISK is attached to

other generation methods or to conservation...", while in 5.25 we have:

> COMPUTER ERROR OPENED ALTA (power station) FLOOD GATES...
> ...three-meter high flood wave... full police rescue alarm...
> warnings to campers etc...

Persons interested in risks of power generation, in a broad sense, might also wish to read Tom Clancy's "Red Storm Rising". The first few chapters are a graphic account of how centralized computer control of oil refineries permits one-man sabotage on a staggering scale. (The rest of the book, which is also quite good but less relevant, is about the Third World War that results when such a single act of sabotage severely disrupts Soviet oil production. This is a risk on a scale that dwarfs most of the RISKS discussions!)

I would also observe that one aspect of energy conservation is efficient, often computerized, management of energy use in large buildings etc. I don't recall hearing of any serious problems with such systems, but surely there must have been some, especially early on? Anybody know?

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

---

Re: Subject: Computer Error Opened Flood Gates of Alta Dam (Norway)

Amos Shapir <nsc!nsta!nsta.UUCP!amos@Sun.COM>

Haavard Hegna <hegna%vax.nr.uninett@NTA-VAX.ARPA> writes:
>The Alta Power Station has been operative since May this year. "The paradox
>is that this very autumn we were going to install a valve that will prohibit
>the accidental opening of the flood gates", the dam administration says.

Installing the safety features a few months *after* the system becomes operational may be called a 'paradox' in Norwegian; the English term is, if I am not mistaken, 'incompetence'. (In Russian it's Chernobyl, of course).

Amos Shapir, National Semiconductor (Israel)
6 Maskit st. P.O.B. 3007, Herzlia 46104, Israel Tel. +972 52 522261
amos%nsta@nsc.com @{hplabs,pyramid,sun,decwrl} 34 48 E / 32 10 N

Re: Another electronic mail risk (Doug Mosher)

Prentiss Riddle <ut-sally!im4u!woton!riddle@seismo.CSS.GOV>
10 Aug 87 15:37:20 GMT

I just wanted to point out that the risk of sending messages to the wrong recipients can apply to paper mail as well as electronic mail. My father claims to have once known a manager who forbade the use of paper clips in his office. It seems that he had once lost a job because a memo critical of one of his superiors got snagged in the paper clip of another memo addressed to the person he was criticizing! :-)

--- Prentiss Riddle

--- Opinions expressed are not necessarily those of Shriners Burns Institute.
--- riddle@woton.UUCP {ihnp4,harvard,seismo}!ut-sally!im4u!woton!riddle

Search RISKS using swish-e

THE RISKS DIGEST

Forum on Risks to the Public in Computers and Related Systems

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

Volume 5: Issue 27

Tuesday, 11 August 1987

Contents

Re: Secrecy About Risks of Secrecy (RISKS-5.26)

Jerome H. Saltzer <Saltzer@ATHENA.MIT.EDU>
Tue, 11 Aug 87 11:55:08 EDT

> From: "Maj. Doug Hardie" <Hardie@DOCKMASTER.ARPA>
> I am not convinced that you can publish overviews that do not provide
> any thoughtful person with enough insight to fairly easily complete
> the details of the attack. I believe that it is the initial
> identification of a flaw that is difficult, not the exploitation of it.

That comment rings completely true. I would argue the following implication: publication of any information about a problem should be accompanied with full detail, so that the good guys have all the information they need to get on top of it. (Security lesson number one: technology transfer to the good guys is an order of magnitude harder than to the bad guys.)

Hardie continues to comment on a comment by our moderator. . .

> [... If a system is fundamentally flawed, it should not be used
> in critical applications where those flaws could result in serious
> compromise... PGN]

> I suspect that removing all sensitive information from critical applications would cripple the government. Also, there is no way to replace all those systems with secure systems in the near future. Even if we only buy secure systems for new applications, it will be several decades before the fundamentally flawed systems are gone.

I think that both of these positions are a little too polar, and thus are dancing around the real-world problem. There are situations when it may be a reasonable risk to leave sensitive information in a flawed system, for example when you are fairly sure that your opponent doesn't yet realize the information is there and probably won't trip over it immediately, or when you are fairly sure that the other side hasn't yet learned of the security flaw. But since knowledge of such things spreads, that kind of decision is very time-sensitive--the risk increases every day. So the decision must be accompanied by a plan to shore things up, either by fixing the flaw, getting the information moved to a safer place, or--a common solution--putting other barriers around the flawed system. Anyone who continues to run a flawed system for years, much less decades, while trying to maintain secrecy about its problems isn't taking a risk any more, he is inviting a disaster.

Jerry

> [The placing of supposed barriers again is subject to the skepticism that Jerry has about the system itself... The problem is recursively unsolvable in any definitive sense, although the perceived risks are often only a shadow of the actual risks. PGN]

"Mustn't tire the computer!"

"A. N. Walker" <anw%maths.nottingham.ac.uk@Cs.Ucl.AC.UK>
11 Aug 87 18:21:26 BST (Tue)

`The Observer' [national Sunday paper] reports on `the nightmare of a woman robbed of 8,750 pounds'. Her Abbey National Building Society [do you have building societies? a sort-of bank with just deposit accounts and mortgage accounts] cash card had been used to steal 250 pounds (the daily limit) per day for 35 consecutive days from her account. The RISKS interest comes from the comment by Abbey National's head of security (i.e., not just a spokesman): "It is true that we tell counter staff at branches to make enquiries if cheques are cashed on three consecutive days. But to instruct the computer to do this on ATMs would be far too time-consuming," he said.

Elsewhere, Abbey National claims to process 5.7M transactions per year; say 15K transactions per day average, perhaps 50K per day peak. I'll leave others to estimate the size of the computer needed to compare three or four 50K-record files within a day, looking for repeated transactions on individual accounts, and the amount of time needed to write the software.

The moral is: don't expect computers to perform all the routine, boring tasks that they do so much better than people.

Andy Walker, Maths Dept, Nottm Univ, UK

Automated environmental control RISKS

Joe Morris (jcmorris@mitre.arpa) <jcmorris@mitre.arpa>
Tue, 11 Aug 87 13:01:37 EDT

In RISKS-5.25, Henry Spencer asks about problems with the computerized environmental/energy controls that are becoming popular in large office buildings. Several years ago (and with a former employer) I had the dubious pleasure of seeing what happens when one of these systems is installed without considering that the building tenants might not fit the 'standard' mold. The building, located on a university campus, housed four floors of professors' offices, a lecture hall, and the computer center. The new environmental control system, which was run remotely from the Physical Plant offices, was retrofitted to the building several years after it was constructed, and was designed for use where the building was occupied during the day and vacant at night. Sure enough...the first night the $%^&* thing turned the air conditioning compressors off at about 19:00, causing all sorts of panic in the computer room. No damage resulted from this (except a few gray hairs), but it highlights the sort of incompatibilities that can result when too many assumptions are made about an environment.

Joe

Social Security Administration -- Inside Scoop

Martin Minow <decvax!LOCAL!minow@decwrl.dec.com>
Tue, 11 Aug 87 19:00:24 edt

Date: 10 Aug 87 23:27:53 GMT
Path: decvax!decwrl!labrea!aurora!ames!amdcad!cae780!ubvax!lance
From: lance@ubvax.UUCP (Lance Keigwin)
Organization: Ungermann-Bass Enterprises

Just after college I accepted a job with the Social Security Admin (SSA) in a NYC district office. I spent several years with SSA as a claims representative, operations supervisor, and regional program specialist. Fortunately I had the good sense to leave several years ago, when it became very clear that federal service was not an alternative to anything.

In these jobs I dealt with all levels of the SS program. Undoubtedly the two biggest headaches for SSA (and the public claimants) were resolving discrepancies in dates of birth and earnings records. Screwups in establishing age is another story, and far less controversial. SSA's record there is really pretty good, if the claims rep is not a dope.

But scrambled earnings records are almost impossible to fix. This usually happens when somehow an employer gets a hold of a wrong number, usually from an employee (although the employer could pick it up from almost anywhere...and they do!). Of course there is cross-checking against what SSA believes is the right name and number but all it takes is some (#$%@$%) clerk to cross refer two numbers to the same person and zap! Suddenly you're record relects someone else's wages too. Or worse:

your covered earnings are credited to some third party. This happens all the time because people forget their numbers, re-apply for a second one, guess wrong, etc. Safeguards exist but if you consider the scale here (all those workers, all those employers, and the general interest of the average gov't employee in doing the job right even if it means more work and worsened processing statistics) there are bound to be major problems.

When does the error come to light to you, John Q. Public? If at all, almost always at retirement, some decades in the future; at a time when many employer records are gone, if not the employer itself, and your recollection is at best fuzzy. Chances are probably 9 in 10 that you'll never get credit for all the taxes you paid, if your record is messed up obviously enough for a rep to notice it and to look into it.

My advice:

1) Never, NEVER give anyone a fake SSN. It will haunt you later in life. If SSA has to search for earnings under a different number (spotted on an application for employment, a credit card report, school record, etc.) you will suffer significant delays in getting your correct benefit at best. More likely, you will never live to see the tax credit.

2) Always, ALWAYS request a statement of your earnings every three years. There are screwy statute of limitations regulations (3 years, 3 months and 15 days), about when an error can be corrected. Also the statement of earnings you get will only breakout the last several years individually, and will total all prior years in one lump sum, so it it good to do it periodically.

3) If you suspect an error, ask for a complete posting of each year (a "certified earnings record"). If you're given a little card to complete and told it will be mailed to you, don't buy it! You can only get a complete record by seeing a Service or Claims representative, who must complete an SSA-450 for transmission to HQ in Baltimore. Insist on a photocopy of it when it arrives. Be troublesome, if necessary.

4) If you do see an error, put your dispute in writing and if you must mail it in, do so certified mail. Establishing the date you first suspected an error is important. SSA has ways of "scouting" an employer's records. Ask to have it done.

5) Check your W-2 for the correct SSN. Paystubs too, but especially the W-2. Report any error to your employer and IRS.

6) If you don't want to give your correct SSN to someone and feel you must fake it, give them a number that starts with "9". There is no such thing as a real 900-series number so you are not risking screwing up yours or someone else's account. SSA will never accept it.

7) If you get an official decision that goes against you, protest if you really believe you're being cheated. There are several appellate steps, and usually the official who decides is reasonably intelligent and responsible. Read the back of the notice about "reconsiderations", "hearings", etc. The reversal rate it very high.

As a matter of interest, two years after I started work for SSA I requested a record of my earnings. Sure enough, there was an error in two quarters. Want to guess who the employer was that messed up? Yep, SSA. It took them 3 years to fix it. Good thing I had an "in". :-)

I also discovered that my retired father should have been getting benefits for three of his student children (an SSA snafu). I had us apply, and asked for full retroactivity (over 8 years). The claims examiner awarded only 12 months of retroactivity. I appealed. We won. Total family benefits came to over $7000. I used my $1500 to buy a washer and dryer.

Lance P. Keigwin (lance@ubvax.UUCP) (408)496-0111 (operator) 562-7738 (direct)
US Mail: Ungermann-Bass Inc, 2560 Mission College Blvd, Santa Clara, CA 95052
UUCP : {ucbvax,decwrl,ihnp4,allegra}!amd!ubvax!lance pyramid!ubvax!lance

---

Fire protection in the computer room

Dave Curry <davy@intrepid.ecn.purdue.edu>
Tue, 11 Aug 87 18:08:47 EST

The discussion of the NASA computer room which got flooded brings this to mind.

Here at Purdue, the University fire department (actually, I think it's the Safety & Security folks) doesn't like Halon systems. Admittedly, there are risks to humans when using Halon systems, since Halon's function is to remove the oxygen from the air. (I have heard stories that some Halon manufacturer placed people in a room full of Halon to prove it was "safe"--not sure I'd want to try that one, although they apparently all survived with no ill effects.)

Anyway, we as computer folks like Halon. Sprinklers tend to have rather adverse effects on the hardware. But, we can't install a Halon system in our computer rooms. We have to install a sprinkler system. So.... we have Halon extinguishers and sprinklers. We haven't had any leaks. Yet. Covers are a neat idea; too bad we don't have any (a risk we probably shouldn't be taking).

The risk here is due to a lack of understanding on the part of people who don't work with the hardware... they don't realize that their aversion to Halon (which is easily countered by having the firefighters wear airmasks) puts several million dollars worth of equipment, not to mention the probably incalculable value of the data stored, at risk.

--Dave Curry, Purdue University

Search RISKS using swish-e

THE RISKS DIGEST

Forum on Risks to the Public in Computers and Related Systems

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

Volume 5: Issue 28

Wednesday, 12 August 1987

Contents

Certification of software engineers

Nancy Leveson <nancy%cb6.uci.edu@ROME.UCI.EDU>
Wed, 12 Aug 87 21:16:16 -0700

I would like to raise the issue in this forum of certification of software engineers. Certainly, someone who has built a model aircraft would not be considered (or consider themself) competent to design a commercial jet. Yet those who have written a few BASIC programs as a hobby often seem to have no such qualms about their education and abilities. High school students tell me about their jobs building important software systems. As a contrast, engineers must usually satisfy minimal educational requirements, and engineering projects for critical systems often have a requirement for a professional engineer to be involved. Although the ACARD report suggestions were regarded as extreme by many in the computer science field, they are not necessarily much more than is routinely expected in other related professions.

For example, System Safety Engineering is a field that is about the same age as computer science or perhaps even somewhat younger. There are, however, already certification programs. And as an example of what can be done for critical systems, there is a MIL-STD-1574A (USAF): System Safety Program for Space and Missile Systems that mandates that Air Force space and missile projects have a "Qualified System Safety Engineer" to manage the system safety program and be "responsible for the effective implementation of the following tasks ... [too many to cite, but essentially the tasks necessary to implement a system safety program]" and who is "directly accountable to the program manager [i.e., the US Air Force program manager] for the conduct and effectiveness of all contracted safety effort for the entire program."

A Qualified System Safety Engineer is defined as someone who must meet the following requirements:

> "A technically competent individual who is educated at least to the bachelor of science level in engineering or related applied science and is registered as a professional engineer in one of the states or territories of the United States or has equivalent experience approved by the Purchasing Office.
>
> This individual shall have been assigned as a system safety engineer on a full-time basis for a minimum of four years in at least three of the six functional areas listed below:
>
> System Safety Management
> System Safety Analysis
> System Safety Design
> System Safety Research
> System Safety Operations
> Accident Investigation

I don't know of any similar requirements in government standards for managers of software engineering programs on critical projects nor any similar assignment and acceptance of direct responsibility and accountability to the customer for the *effectiveness* of the software engineering effort. Does anybody else? Am I wrong in my observation that under-qualified people are sometimes doing critical jobs and making important decisions? Do you

agree that some type of certification is necessary? If so, there are still many open issues e.g., should there be minimum educational requirements and what kind, should there be minimum experience requirements, should there be examinations, should certification be in particular application areas (dp, scientific, safety-critical real-time, etc.) or perhaps in particular subareas (systems analysis, design and coding, QA, etc.), should there be continuing education requirements, should there be minimum requirements for those teaching software engineering and certification of educational programs, ...

Nancy Leveson

Re: Secrecy About Risks of Secrecy (RISKS-5.26)

"Maj. Doug Hardie" <Hardie@DOCKMASTER.ARPA>
Wed, 12 Aug 87 12:46 EDT

> From: Jerome H. Saltzer <Saltzer@ATHENA.MIT.EDU>
> So the decision must be accompanied by a plan to shore things up, either
> by fixing the flaw, getting the information moved to a safer place, or--
> a common solution--putting other barriers around the flawed system...

This is practical when you are dealing with a single system. However, the number of DEC VAXs (as an example) that handle sensitive information is too large to identify. There currently exists no way to even tell all the administrators using any particular system that they have a problem. While additional barriers are probably not prohibitive for one system, when multiplied by the number of systems in use throughout the government, I expect that cost would be unbearable.

-- Doug

[... and the cost of each administrator and user on each system keeping his head in sand may be even greater... PGN]

<ucbcad!ames.UUCP!lll-tis!elxsi!beatnix!rw@ucbvax.Berkeley.EDU>
Tue, 11 Aug 87 08:18:31 pdt

(Russell Williams)
To: ames!CSL.SRI!RISKS@csl.sri.com
Subject: Secrecy of Secrecy: A vote for disclosure

I just want to vote, very strongly, for disclosure of operating system security flaws. Non-publication of these flaws assumes that there is some other system for distributing such information only to those of us in industry responsible for design and implementation of reasonably secure operating systems. If there is such a system please let me in on it (after a suitable security check, of course); if not, I'm confident our customers would prefer the situation where 10 potential penetrators *and* I know the information, to the situation where only 5 potential penetrators know it.

Russell Williams, ELXSI Super Computers, San Jose
...{ucbvax!sun,lll-lcc!llll-tis,altos86}!elxsi!rw

---

security discussions

<putnam%thuban.tcpip@ge-crd.arpa>
12 Aug 87 11:42 EST

The question about open discussion of computer security flaws brings up an interesting point that I have not seen mentioned, that is, that the people who understand such flaws (often the people who try to find them) are not as often as we might like the people who administer the systems. In many cases I have seen the systems managers are not prepared, either by interest, temperament, or background, to understand the security problems and react properly to them. (Not that this is the case everywhere, but it is certainly the case in many situations.)

Such system managers are the types who tend to react to security holes by trying to suppress any information about them - not by trying to fix them. They are also quite likely to respond inappropriately by imposing severe security measures in the wrong places - usually impeding the real purpose of the machines, and rarely actually fixing the problems (indeed, sometimes this "added security" makes the problem worse).

The question of publicizing security holes is thus further complicated. If the problem is publicized, will it spur some people to take (often inappropriate) measures that will inconvenience (or worse) the users of the machine in a misguided attempt to patch the problem?

jeff putnam

[We have also had various cases of people who tried vainly to convince their administrators that there were problems, and then got fired when they demonstrated the problems... PGN]

Eliminating the Need for Passwords

Lee Hasiuk <ucbcad!ames.UUCP!rochester!srs!lee@ucbvax.Berkeley.EDU>
Wed, 12 Aug 87 10:07:33 EDT

Without trying to continue the discussion on passwords, access codes, credit card numbers, etc, I would like to relate a very interesting article about eliminating the need for people to ever put their actual code in the open. The article was about 'Zero Knowledge Proofs' and appeared in the Science Times section of the New York Times earlier this year.

It appears that an Israeli scientist has developed an authorization system based on such proofs that allows a person to verify that they are the owner of an account, without having to give away the 'account number' or any other information which allows them to be impersonated. The basic idea is to give the account owner a complex graph which is successfully colored so that

no two connected nodes use the same color. It is easy to generate such a graph, but given a complex graph, coloring it is not, in general, possible to color it successfully.

A device checking authorization gets to see the graph, but the color of the nodes is hidden. The device picks two connected nodes at a time and is shown that they are, indeed, colored differently. After each pair has been shown, the colors used in the graph are interchanged so that after many tries the device can be quite sure that the graph is colored, but have no clue as to a coloring scheme that works (which when combined with the graph, represents the actual account number).

The article stated that such a scheme could be applied to passwords, and hypothesized a computer that, rather than ask for a login password, asked a series of questions that would change each session. The user would know a scheme, based on the questions and his 'password' to produce answers that would let the computer know with very high certainty that they were the authorized user.

Lee Hasiuk

[Also note crypto authenticators such as the Sytek Challenge mechanism. But also note that access has been gained, some underlying operating systems may force you to assume that everyone is equally trusted (or untrusted)... PGN]

Re: Risks of automating production

Richard A. Cowan <COWAN@XX.LCS.MIT.EDU>
Mon 10 Aug 87 03:47:58-EDT

> From: "James H. Coombs" <JAZBO%BROWNVM.BITNET@wiscvm.wisc.edu>
> The folklore has always been that computers, especially in the form of robots, would one day render blue collar workers obsolete...

It is true that automation has not rendered workers obsolete, or resulted in huge cost savings. As you note, the main impact of automation so far is that it results in greater central *control* over the production process. In fact, this was one of the principal motives for automation from the start: management wanted greater control over labor. (By "management" here I mean high-level managers who are removed from day-to-day production.)

Even though the worst fears have not been realized yet, that is no reason to be optimistic. Although automation thus far has been rather awkwardly implemented (requiring nearly as many workers as before), it has set the stage (by routinizing work and thus deskilling workers) for a new phase in automation that actually gets rid of the work force. As David Noble said in his (highly recommended) book Forces of Production, "Men behaving like machines paved the way for machines without men."

> ... The speculation now is that managers are more likely to be displaced than workers, since it is the managers who tend to be responsible for inventory management and accounting.

The "managers" to be replaced here are probably quite low-level supervisors. But the idea that automation hurts management *in general* (while the workers make out fine) would be a bit silly. In the end, I believe that automation will cause incredibly disruption and suffering unless there is also a dramatic shortening of the work week.

Check out the Noble book -- Oxford University Press, 1984!
-rich

Re: Risks of automating production

"James H. Coombs" <JAZBO%BROWNVM.BITNET@wiscvm.wisc.edu>
Mon, 10 Aug 87 13:09:17 EDT

> From: Richard A. Cowan <COWAN@XX.LCS.MIT.EDU>
> Although automation thus far has been rather awkwardly implemented
> (requiring nearly as many workers as before), it has set the stage
> (by routinizing work and thus deskilling workers) for a new phase in
> automation that actually gets rid of the work force.

I have been confused from the beginning about what it is that the workers do now. I suppose that it could be little more than filling parts buckets for machines or something like that, in which case their work would be even more routine than before. I had this hope, however, that they were servicing the machines, in which case their work might be significantly more skilled and interesting. Can anyone give more details on this?

Also, I wonder what happens to the managers at various levels. Does their work become more interesting and rewarding, or less? I'm sure that for some, the "planners," work becomes less stressful. What about the others?
--Jim

'Mustn't tire the computer!'

Scott E. Preece <preece%mycroft@gswd-vms.Gould.COM>
Wed, 12 Aug 87 09:34:52 CDT

> "A. N. Walker" <anw%maths.nottingham.ac.uk@Cs.Ucl.AC.UK>
> "It is true that we tell counter staff at branches to make enquiries if
> cheques are cashed on three consecutive days. But to instruct the
> computer to do this on ATMs would be far too time-consuming," he said.

Well, while it's true that it shows great lack of insight not to do anything about a known potential problem (especially when the withdrawals were at the daily max, which should always be a flag for caution), it's less than clear what they should do. A human teller can ask for ID; most existing ATMs can't. If you just fail the transaction, you're going to make customers unhappy (how often we object to restrictions intended to protect us). It would be a good idea for all ATMs to have cameras and for human intervention to be triggered by any of a number of suspicious circumstances (I'd say max

withdrawals on two successive days was suspicious), but that's also going to raise the cost of service...

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

> ["The real risk here is having people who do not know anything make pronouncements about what computers can and cannot do, including the bank manager... Why would anybody store the information unsorted and unorganized and then search brute force through every record?!" ... anonymous commenter on Andy Walker's message]

Re: "Mustn't Tire the Computer"

Kuhn <kuhn@ICST-SE.ARPA>
Wed, 12 Aug 87 10:45:24 edt

[...] When I worked on ATM and systems software for banks and savings & loans, [for UK readers: US savings & loans are descendents of your Building Societies] I learned that some of them run what they call a "Kiting Suspect Report" that attempts to spot check kiting schemes. One of my customers detected a check kiter three or four days after he had started cashing 8-10 checks a day at area supermarkets against his accounts at my customer and another S&L. I don't know if charges were ever filed, but the other S&L and all the supermarkets were notified and the scheme stopped.

--Rick Kuhn, National Bureau of Standards

Re: NASA wet computers

Eugene Miya <eugene@ames-nas.arpa>
Tue, 11 Aug 87 23:43:31 PDT

[...] Practically, all of major computing computing facilities in NASA (not the really small distributed machines) have wet covers. This is because most Centers were constructed before halon was put to wide use and so fire protection is provided via "wet" protection. The problem comes in upgrade. Mission Control Centers are used practically all the time, making upgrades tough. I asked this question at a meeting today for RISKS. It comes from "very reliable sources."

Also note that lots of Centers are in hurricane areas as well.

--eugene

Halon risks in computer rooms, etc.

Dave Platt <dplatt@teknowledge-vaxc.arpa>
Wed, 12 Aug 87 10:43:35 PDT

> [Many messages on this subject... I have excerpted to reduce overlap. PGN]

As I understand it, Halon's fire-killing ability comes from two characteristics of the gas:

1) It excludes oxygen, when used in sufficiently large amounts. This is one of the ways in which carbon dioxide kills flames (its cooling effect being the other), and thus any oxygen-exclusion risks from a Halon system would also probably exist in a CO2 system of similar gas-magnitude.

2) Halon interferes, chemically, with the combustion process. I believe that it ties up the free (ionized) radicals in the flame, and blocks one or more of the partial-oxidation steps. Because this is a chemical effect, and not a physical one such as oxygen exclusion, it can occur at relatively low concentrations of Halon in the atmosphere.

I saw a demo at NCC a couple of years ago, in which a Halon-system manufacturer's sales-rep stood in a closed booth smoking a cigarette. He then let loose a 1-second burst of Halon, and the cigarette went out. For the next several minutes, he stood in the booth, breathing normally, and demonstrated that he was unable to relight his cigarette (he stuck a Bic lighter outside the booth through an arm-sized hold, flicked it alight, moved it gently back within the booth, and it went out the moment it entered the Halon-charged atmosphere).

I've been told that the major risk to humans from being in an area that has been Halonized isn't the Halon itself... instead, it's the risk of inhaling the rather nasty partial-combustion products of the plastics, other petrochemicals, and miscellaneous combustibles that were burning when the Halon was released. Because the combustion was interrupted, these chemicals won't have been burned to completion (to water, carbon dioxide, etc.); they may include lots of carbon monoxide, hydrochloric or other acids, and similar things that aren't conducive to long life and respiratory health.

Please don't take this as gospel... and kids, don't try this at home.

X-Uucp: /decwrl|hplabs \
{ seismo|uw-beaver}!teknowledge-vaxc.arpa!dplatt
\ucbvax|sun /
X-Usnail: Teknowledge Inc., 1850 Embarcadero Road, Palo Alto CA 94303
X-Voice: (415) 424-0500

HALON

<uwvax!seismo!ingr!tesla!steve@ucbvax.Berkeley.EDU>
Wed, 12 Aug 87 11:57:41 EDT

Several years ago, at a previous employer, I designed fire control systems, including many HALON systems. HALON does -not- extinguish the fire by displacing the oxygen in the air. It interferes with the actual

combustion process. The amount of HALON required to disable combustion is only around 3%-7%, which leaves plenty of oxygen for humans. (The following is all from memory and may not be entirely accurate) There are some effects to humans from prolonged (>1 hour) exposure to HALON at this concentration. I think that they are on the order of headaches, etc. and dissappear when exposure ceases. There were no long term effects known at that time.

The greatest danger in using HALON that I know of results from exposure to the gas as it is discharged from the nozzles into the room. HALON systems are designed to get the gas dispersed in the required concentration as rapidly as possible. The high flow rate of the gas and the expansion at the nozzle results in very low temperatures in the discharged gas. I heard a story that a government agency required a full discharge test of a HALON system in a computer room, and to shield some installed equipment, someone held a sheet of plywood between one of the nozzles and the equipment. He suffered severe frostbite on all eight fingers.

Steve Conklin, Intergraph Corp., Huntsville, AL 35807, (205) 772-6618
{uunet,ihnp4}!ingr!tesla!steve

---

halon, sprinklers, etc.

Jack Ostroff <OSTROFF@RED.RUTGERS.EDU>
12 Aug 87 11:48:01 EDT

I used to be a volunteer fireman when Halon became popular, [...]

At one computer center I know, the fire extinguisher system consists of CO2 jets below the artificial floor. It has never gone off, but rumor has it that the jets will throw the floor tiles a small way, before flooding the entire basement with CO2 in several minutes. This DOES replace the oxygen, and everyone who works there is told to RUN LIKE HELL if they hear the fire alarms go off.

Jack (OSTROFF@RED.RUTGERS.EDU or ...!rutgers!red.rutgers.edu!ostroff)

Halon to protect computer installations

"LT Scott A. Norton, USN" <4526P%NAVPGS.BITNET@wiscvm.wisc.edu>
Wed, 12 Aug 1987 15:10:03 PDT

[...] Of course, Halon does have some risks. Nothing's perfect. The immediate risk to people is that at very high temperatures, Halon is chemically changed to phosgene, a strong poison that burns the lungs. The temperature in a small class-A fire in a computer room would not produce hazardous amounts of phosgene, but a large conflagration might.

The reason why the fire department is not satisfied with just Halon is that it is a one-shot system. That's O.K. if a fire breaks out in the protected area, the Halon system activates promptly, and the fire goes out. But there are some failure modes:

1. If the room is not sealed, the Halon will be blown away. If the initial source of combustion is still present, the fire will reflash. Normally, Halon systems shut off ventilation and air conditioning before discharging the Halon, but do you trust those relays to work?

2. If the fire spreads to the area from outside, the Halon system will only push it back once. Once the Halon dissipates, the fire can move in again.

3. Halon systems are complicated. Contrast that with a sprinkler system: Water in a pipe, Wood's metal keeping it there. In a fire, the metal melts and water sprays out.

So, the tradeoff in computer room fire protection is that Halon is very safe to the equipment and to people in the event of an accidental discharge, sprinklers are safe for the people but not the equipment in an accidental discharge. In a small fire under normal conditions, Halon is effective at extinguishing the fire but doesn't hurt the equipment and has a low risk to the people (probably lower than that of the carbon monoxide from the fire). But in the case of a big fire, Halon by itself can not be counted on to fully extinguish the fire.

When I was Tactical Data Systems Officer on a cruiser, I worried about firefighting water, since the Navy uses sea water to fight fires. So don't complain about fresh water spraying into your equipment, it will just wash troublesome dust off the circuits. :-)

LT Scott A. Norton, USN
Naval Postgraduate School
Monterey, CA 93943-5018
4526P@NavPGS.BITNET

Fire protection in the computer room

Scott E. Preece <preece%mycroft@gswd-vms.Gould.COM>
Wed, 12 Aug 87 09:45:10 CDT

[...] We had a false alarm set off the halon in our machine room. The amount of warning the system gives before discharging the gas is impressive. So is the effect on the computer room (lots of gas, lots of air motion, lots of dust and displaced ceiling tiles). Much preferable to water. (But also much more expensive -- that false alarm was not cheap by any stretch of the language.)

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

---

railway automation

Stephen Colwill <mcvax!praxis!steve@seismo.CSS.GOV>
Wed, 12 Aug 87 11:09:00 WET

> Scott E. Preece <preece%mycroft@gswd-vsm.Gould.COM>
> A train is a large object whose position is only approximately known
> at best, whose speed is hard to change and is changed using systems
> whose performance is subject to wild fluctuations with age, maintenance
> and track conditions, and whose surroundings are totally invisible to
> the controlling system.

In the context of the automation of an existing network using old rolling stock, I take your point. My original posting focussed, however, on the London Docklands Light Railway. The LDLR was purpose-built from scratch, the rolling stock is new and also purpose-built. It seems to me that the designers had ample opportunity to install precisely the kind of sensors you describe. I cannot believe that these sensors are beyond modern technology.

Stories of trains jumping buffers give the lie to any hope that the opportunity afforded by the design of a virgin system has been properly taken. It is this that I find so disappointing.

Steve Colwill, Praxis, Bath.

Employment opportunities at MITRE

Marshall D. Abrams <abrams%community-chest.mitre.org@gateway.mitre.org>
Wed, 12 Aug 87 15:40:37 -0400

We are looking for for people to join the Information Security Group at The MITRE Washington Center. As you probably know, MITRE is a not-for-profit Federal Funded Research and Development Center, founded at the request of the Air Force. We work almost exclusively for the government, both for civil and military agencies and departments.

MITRE support to sponsors includes: security requirements analysis and definition; security assessment of existing systems; information security design; procurement support including document development, evaluation, and contractors supervision; policy development support; prototype implementation; verification; and certification and accreditation planning. We have a good mix of theory, policy, and real applications which has proven to be very synergistic. We are currently involved with network and database security both for development of evaluation criteria, and for applications to operational systems.

I would welcome the opportunity to discuss our work program, and staffing requirements with people at all levels of qualifications. U.S. citizenship is required.

Marshall D. Abrams, phone: (703) 883-6938, The MITRE Corporation, 7525 Colshire Drive, Mail Stop Z670, Mc Lean, VA 22102

Report problems with the web pages to the maintainer

Search RISKS using swish-e

THE RISKS DIGEST

Forum on Risks to the Public in Computers and Related Systems

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

Volume 5: Issue 29

Saturday, 15 August 1987

Contents

RISKS submissions

Peter G. Neumann <Neumann@csl.sri.com>
Sat 15 Aug 87 18:12:52-PDT

I submit that your submissions over the past weeks have driven me into submission. The quality of contributions and self-control exhibited by contributors has dropped off radically. Various complaints have been received recently that I have suddenly become far too generous in including too much irrelevant, unsound, incoherent, and otherwise marginal material. Well, I currently have a HUGE backlog of messages for consideration -- 30 in the last four days -- but all are mostly minor variants of previous contributions, and many of them will not emerge. (Perhaps the recent deluge is merely a summertime phenomenon?) Well, due to my own heavily overloaded schedule, RISKS will slow down for the next two weeks, when I will be limited to a few short shots at NETland. But please keep on submitting the GOOD stuff -- I'll get to it eventually. And please excuse the slowdown.

By the way, I erred in including the MITRE notice in RISKS-5.28. Please don't expect me to do it again.

The responses to Denning/Saltzer/Hardie are running about three-to-one for

nonsecrecy about security flaws, with all sorts of caveats, hedges, special cases, etc. Logic tells you that you'd better know when -- and how -- YOU are vulnerable.

The certification issue is not generating much enthusiasm either way. (Perhaps certification is also needed for computer system users who have authorization to do act dangerously or fraudulently.) The legal aspects of screwing up may be a driving force toward certification to protect system developers (or procurers?) if a big liability suit gets won by the injured parties. (The Rogan case that follows is small potatoes. By the way, Donn Parker notes that the Equity Fund case, with direct losses of $200 million, is actually estimated at $2 billion total losses if indirect costs such as stockholder losses are included.)

The standards issue for system safety is warming up again, but is also not likely go generate too much enthusiasm. (If you care, see the concluding item in this issue. It also implies all sorts of risks.)

Lack of user training = legal liability?

Rodney Hoffman <Hoffman.es@Xerox.COM>
14 Aug 87 11:07:01 PDT (Friday)

[Also submitted by Frederick Bingham]

Excerpted from the Los Angeles Times, Aug. 13, 1987:

COMPUTER SNAFU RULED A RIGHTS VIOLATION
Wrong Man Repeatedly Detained on Murder, Robbery Charges
By Jack Jones

The Los Angeles Police Department violated the constitutional rights of a Michigan man by continuing to list him in a nationwide crime information computer system as wanted for murder and robbery, even after it was clear the real suspect was using his name, U.S. District Judge Robert Kelleher has concluded.

Terry Dean Rogan, 29, will now go to Los Angeles Federal Court to seek monetary damages .... Kelleher found that [the two] Los Angeles Police Detectives... do not share liability with the city, even though on several occasions they re-entered Rogan's name in the National Crime Information Center system and failed to add new descriptive information that would have established Rogan as the wrong man.

The city failed, Kelleher ruled, to properly train and supervise the officers in the constitutional protection aspects of using the crime center system and the necessity of adding more accurate information when it becomes available. The actual suspect, Alabama state prison escapee Bernard McKandes,... began passing himself off as Rogan in 1981....

Rogan ... was first arrested in October, 1982.... He was held in jail until a fingerprint check showed he was not the man being sought.

Nevertheless, ... Los Angeles detectives put his name back into the computer, neglecting to add qualifying information, and he was arrested four more times -- mostly after routine traffic stops. On two occasions, he was taken into custody at gunpoint, handcuffed and jailed. It was not until early 1984 that Rogan's name was removed from the computer system -- after a Saginaw News reporter told [one of the L.A. detectives] that McKandes ... was back in prison in Alabama. McKandes... subsequently was convicted of the California murder and robbery charges.

[See ACM Software Engineering Notes 10 3 (July 1985) for some further background. PGN]

London Docklands Light Railway; Northern Line's Dot-Matrix Indicators

Mark Brader <msb@sq.com>
Thu, 13 Aug 87 12:44:03 EDT

The June issue of the British magazine Modern Railways carried this item:

> 'UNAUTHORISED TESTS' CAUSED DLR CRASH
>
> The Managing Director of Docklands Light Railway Limited, Cliff Bonnett, has said the accident which occurred at Island Gardens station on 10 March (Modern Railways, May) was primarily caused by unauthorised tests, carried out before required modifications had been carried out at the southern terminus. The train, which ended up overhanging from the elevated track after crashing through buffers, would have been 'arrested' if the protection system 'in its full and modified form' had been installed. The train was being driven manually.

Incidentally, on the same page of the magazine is this:

> DOT MATRIX PROBLEMS
>
> A marked improvement in the performance of the Northern Line's gremlin-infested dot-matrix train indicators is promised by the autumn, but modified software cannot be satisfactorily commissioned for a year, says London Underground, while a new central computer at the line's Coburg Street, Euston control centre is awaited. Meanwhile, some indicators have lost the minutes-to-train-arrival feature, displaying only the order of train arrival.

Mark Brader, Toronto, utzoo!sq!msb

Software and system safety

Nancy Leveson <nancy@commerce.UCI.EDU>
Thu, 13 Aug 87 10:49:41 -0700

Two weeks ago I taught a 3-day continuing education class on software safety at UCLA. The makeup of the class says some interesting things about the

awareness of software safety issues in the U.S. I was pleasantly surprised to have 40 people enrolled (the average class size of software engineering classes there is about 25). Half the class was from outside California which means their management was willing to invest money in sending people across the country to take the class (implying some awareness and commitment to the problem -- the class itself also was not cheap). It was also interesting to note that although the majority of people came from the aerospace industry (including someone from Morton Thiokol), there were 3 medical device manufacturers (all said that their attendance was directly related to the Therac 25 incident -- these accidents that you read about in risks do have an effect, especially when lawsuits and media publicity are involved); 2 commercial aircraft manufacturers and a manufacturer of aircraft engines; the Air Force, Army, and Navy; a couple of firms that do safety analysis on a contract basis; and one in entertainment (Walt Disney).

Many in the class identified themselves as safety engineers [see the following message], but there were also software engineers and a fair number of people who identified themselves as "software safety engineers" or "software system safety engineers." I was especially curious about the software safety engineers and asked a few questions. All but one had previously been system safety engineers and had acquired this title within the past few months. One had been a software engineer previously and had become a "software safety engineer" very recently.

Nancy Leveson

[Now I know where all the mickey-mouse computer systems are coming from. PGN]

New safety MIL-STD

Nancy Leveson <nancy@commerce.UCI.EDU>
Thu, 13 Aug 87 13:31:50 -0700

> [This item may be boring to some of you, and important to others. It is included for the record. Comments To: nancy@ics.UCI.EDU, Cc:RISKS. PGN]

A new change notice to a system safety standard (MIL-STD-882B: System Safety Program Requirements) has just been released (July 1, 1987). The surprise is the amount of reference to software contained in it and the new tasks on software safety included. The following are some excerpts (there is lots missing). I am sending more information to Peter Neumann for inclusion in the next issue of SEN. I am curious about how most system safety engineers, who are untrained in software engineering, will be able to accomplish these tasks. Since in most cases they will not, I would guess that many of these requirements will be passed along to the software engineers to actually perform. The tasks could potentially also have other impacts on software engineers working on safety-critical projects. Those of you in the aerospace industry should be aware of what is about to hit you and others may find other government agencies following suit.

TASK 202 - PRELIMINARY HAZARD ANALYSIS
[includes] consideration of the potential contribution by software to subsystem/system mishaps, safety design criteria to control safety-critical

software commands and responses and appropriate action to incorporate them in the software specifications, and software fail-safe design considerations.

TASK 203 - SUBSYSTEM HAZARD ANALYSIS
identify all components and equipments, including software, whose performance, performance degradation, functional failure, or inadvertent functioning could result in a hazard or whose design does not satisfy safety requirements.

TASK 204 - SYSTEM HAZARD ANALYSIS
perform and document a system hazard analysis to identify hazards and assess the risk of the total system design, including software, and specifically of the subsystem interfaces.

TASK 204 OPERATING AND SUPPORT HAZARD ANALYSIS
requirements to evaluate hazards resulting from the implementation of operations or tasks performed by persons ... Includes identification of changes needed in software to eliminate hazards or reduce their associated risks along with warnings, cautions, and special emergency procedures including those necessitated by failure of a software-controlled operation to produce expected and required safe result or indication.

TASK SECTION 300 - SOFTWARE SYSTEM SAFETY
[states that] Software System Safety is an integral part of the total System Safety Program. The 300 series of tasks are recommended for programs which involve large or complicated software packages ...

TASK 301 - SOFTWARE REQUIREMENTS HAZARD ANALYSIS
The contractor shall examine systems and software requirements and design in order to identify unsafe modes for resolution, such as out-of-sequence, wrong event, inappropriate magnitude, inadvertent command, adverse environment, deadlocking, failure-to-command modes, etc. ... Software Safety Requirement Tracking ... Analyze Software Requirements Specifications:... assure that the System Safety Requirements are correctly and completely specified, that they have been properly translated into software requirements, and that the software safety requirements will appropriately influence the software design...
The contractor shall develop safety-related recommendations, and design and testing requirements and shall incorporate them in the Software Top-Level and Software Detailed Design Documents, and the Software Test Plan.

TASK 302 - TOP-LEVEL DESIGN HAZARD ANALYSIS
... analyze the Top-Level Design ... include definition and subsequent analysis of Safety-Critical Computer Software Components (SCCSC), identify the degree of risk involved, and the design and test plan to be implemented ... ensure that all safety requirements are correctly and completely specified in the Top-Level design. ... include analysis of input/output timing, multiple event, out-of-sequence event, failure of event, wrong event, inappropriate magnitude, adverse environmental, deadlocking, hardware sensitivities, etc.

TASK 303 - DETAILED DESIGN HAZARD ANALYSIS
...shall analyze the Software Detailed Design ... to verify the correct incorporation of safety requirements and to analyze the safety-critical CSCs ... includes relationships between safety-critical and other designated software at the CSCI, CSC, and lower unit levels (including subroutines, data bases, data files, tables, and variables). It also includes the

requirement to include safety-related information in the Software User's Manuals.] ... the contractor shall identify safety-critical computer software units to the code developers, and provide them with explicit safety-related coding recommendations and safety requirements from the top-level specifications and design documents.

TASK 304 - CODE-LEVEL SOFTWARE HAZARD ANALYSIS
The contractor shall analyze program code and system interfaces for events, faults, and conditions which could cause or contribute to undesired events affecting safety... Analyze (1) safety-critical CSCs for correctness and completeness, and for input/output timing, multiple event, out-of-sequence event, failure of event, adverse environment, deadlocking, wrong event, inappropriate magnitude, hardware failure sensitivities, etc. ... (4) proper error default handling for ... inappropriate or unexpected data in the input data stream, (5) fail-safe and fail-soft modes, (6) input overload or out-of-bound conditions.

TASK 305 SOFTWARE SAFETY TESTING
The contractor shall test the software to ensure that all hazards have been eliminated or controlled to an acceptable level of risk. Implementation of safety requirements (inhibits, traps, interlocks, assertions, etc.) shall be verified. The contractor shall verify that the software functions safely both within its specified environment, and under abnormal conditions.

TASK 306 - SOFTWARE/USER INTERFACE ANALYSIS ...

TASK 307 - SOFTWARE CHANGE HAZARD ANALYSIS
The contractor shall analyze all changes, modifications, and patches made to the software for safety hazards, to include the following: All changes to specifications, requirements, design, code, systems, equipment, and test plans, descriptions, procedures, cases, or criteria shall be subjected to software hazard analysis and testing, unless it can be shown to be unnecessary due to the nature of the change... the contractor shall show that the change or patch does not create a hazard, does not impact on a hazard that has previously been resolved, does not make a currently existing hazard more severe, and does not adversely affect any safety-critical computer software component or related and interfacing code... The contractor shall review the affected documentation, and ensure that it correctly reflects all safety-related changes made.

Search RISKS using swish-e

THE RISKS DIGEST

Forum on Risks to the Public in Computers and Related Systems

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

Volume 5: Issue 30

Friday, 21 August 1987

Contents

Role of NISAC in Reporting Vulnerabilities

Bruce N. Baker <BNBaker@KL.SRI.Com>
Tue 18 Aug 87 14:30:40-PDT

In all the discussions that have taken place since Peter Denning's submission about the paradox of reporting vulnerabilities in computer systems, I have been surprised that no one has mentioned DoD Instruction 5215.2, dated September 2, 1986, "Computer Security Vulnerability Reporting Program (CSTVRP)"

The Instruction:

1. Establishes a Computer Security Technical Vulnerability Reporting Program under the direction of the National Security Agency, National Information Security Assessment Center (NISAC).

2. Establishes procedures for reporting all demonstrable and repeatable technical vulnerabilities of Automated Information Systems (AIS).

3. Provides for the collection, consolidation, analysis, reporting or notification of generic technical vulnerabilities and corrective measures in support of the DoD Computer Security requirements in DoD Directive 5200.28, "Security Requirements for Automatic Data Processing (ADP) Systems,"

December 18, 1972.

4. Establishes methodologies for dissemination of vulnerability information.

Some pertinent excerpts are as follows:

...

The program shall be focused on technical vulnerabilities in commercially available hardware, firmware and software products acquired by DoD...

...

The reporting portion of the program is also available on a voluntary basis for the non-DoD AIS community.

...

The NISAC shall maintain a central repository of computer vulnerability information.

Information on the technical vulnerabilities of AIS's shall be protected from unauthorized disclosure while ensuring it is disseminated to individuals responsible for the security of an AIS.

...

The NISAC shall:

...

Establish procedures to encourage the voluntary submission of technical vulnerability information from non-DoD AIS users.

Establish and maintain a data base of technical vulnerability information having security commensurate with its sensitivity.

Establish procedures for transmitting technical vulnerability information to affected manufacturers for corrective action.

...

Vulnerability summaries in narrative form should be addressed to:

National Security Agency
Ft. George G. Meade, MD 20755-6000
Attn: Chief, S2

An inner envelope should be marked:

Attn: CSTVRP/S2093

...

Any technical vulnerabilities in products appearing on the Evaluated Products List will be referred to the responsible vendor for correction. Appropriate warnings will be disseminated.

...

Vendors may be provided the technical details of reported vulnerabilities to make corrections, but shall not be provided information about the specific site(s) concerned, methods of discovery, or other information which could lead to increased site vulnerability without the express written approval of the Head of the DoD Component or the DAA.

Comments: It should be noted that this Instruction applies primarily to systems that have been evaluated against and certified to be technically compliant with the DoD Trusted Computer System Evaluation Criteria (the Orange Book) and, of course, is directed primarily to Defense related agencies. Nonetheless, I assume that they wish to receive vulnerability information on any commercially available product. All vulnerability information received under the instruction is classified at least CONFIDENTIAL so that affects the way the information is transmitted to NSA, especially for any organizations authorized to handle classified information.

A copy of DoD Instruction 5215.2 can be obtained from:
U.S. Naval Publications and Forms Center
5801 Tabor Ave. Attn: Code 301
Philadelphia, PA 19120
Telex # 834295; Phone # (215) 697 3321

[The CONFIDENTIAL aspect is of little help to most RISKS readers, and probably explains why nothing has appeared here before. But there are unclassified evaluations, and the Evaluated Products List is worth noting. In particularly, it contains evaluations of Gould's UNIX-based system UTX/32S and VAX VMS 4.4, for example. A very useful article for people interested in UNIX vulnerabilities and how Gould has sought to fix them is Gary Grossman's "Gould Computer Systems Division Secure UNIX Program Status", 9th National Computer Security Conf., NBS, Gaithersburg MD, September 1986, Addendum pp 27-37. I get a lot of requests for the kind of information found in that article, so I thought I might as well mention it here. (The 10th National is coming up in Baltimore, 21-24 September 1987.) PGN]

Indemnification of ATC manufacturers

<cmpuchm@lll-winken.arpa>
Mon, 17 Aug 87 11:23:32 pdt

The July 20 issue of AW&ST had an editorial viewpoint from a former FAA offical describing a situation where manufacturers of air traffic control equipment are shying away from bidding on ATC contracts because of the large and vague liability issues. This industry has formed a group to try to define liability and provide indemnification. This example reflects the more general situation where the liability risks of 'doing business' will prevent automation in a growing number of 'critical application' industries. As the liability issue comes to a head in other industries we will have a situation where the non-use of computers, instruments, and software will increase the risks to society.

We are and should be responsible for our actions and products as computer professionals. But if liability is undefined and indemnification non-existent, how many of us will be willing to work on 'critical' applications, when our companies, jobs, etc. are 'on the line' owing to potential errors or negligence of third parties, in addition to our own errors or omissions.

Bill Buckley, Compuchem, Inc., Hayward, CA. ATT : 415/489-6514
{lll-lcc,wucs1,uwvax,pryamid,isis,princeton,uunet}!lll-winken!cmpuchm

---

Bank Computers and flagging

Joseph I. Herman (Joe) <DZOEY@UMD2.UMD.EDU>
Sun, 16 Aug 87 14:13:06 EDT

I have been reading with interest (no pun intended) the stories of ATM problems. I find that the data processing problems of the bank I deal

with, 1st National, are not confined to their ATM system (which has actually been extremely reliable). The day before I went on vacation, I transfered some money between a couple of my accounts. I did this the old fashioned way. I walked into the bank, sat down at one of the bank officer's desks and filled out the paper work to transfer funds between accounts. I then went merrily on vacation. When I returned, I found that the funds had been withdrawn from one account and (according to my ATM card) had never appeared in my other account. I went in and talked to the bank manager. They produced a printout of my account and it showed the money was there. Feeling a bit foolish, I thanked them and went back out to the ATM machine. The ATM still showed the balance as being off. I went back to the bank manager and she looked more closely at the printout. What happened is that when the bank officer tried to post my transaction, the computer went down. This caused the transaction to be what they called "double flagged". Withdrawls are always instantaneous, but deposits and transfers take a day to clear. When the transaction was double flagged, the money never got posted. It was still my money and it was in the account earning interest, but I couldn't get to it. That's why the ATM reflected a lower balance since ATM's reflect the balance available, not the actual balance.

I asked the bank manager if I had to come in personally to the bank every time their computer crashed to check my account. She said no, double flags usually expire in 48 hours. For some UNKNOWN reason, they don't always expire. I asked what would have happened if I hadn't come in. She said that the money would have stayed in my account earning interest, but I would never have been able to access it. I asked her why such exceptions like mine (double flagged for > 100 hours) weren't noted. She said it doesn't occur often enough for them to check for the condition.

Personally, I always thought that's what was so nice about computers. They can check lot's of things very quickly and note extreme cases that a human being might miss. And what really got to me is that they (the bank manager and apparently the programming department) DON'T KNOW why some double flags are never removed. That really worries me. I think someone in their programming department should be shot.

Warily yours, Joe Herman

Re: Certifying Software Engineers

Nancy Leveson <nancy@commerce.UCI.EDU>
Thu, 13 Aug 87 16:15:48 -0700

[From Mark Weiser, weiser.pa@Xerox.COM]
The article by Nancy Leveson about certifying software engineers mixes apples and oranges a bit. The first part talks about safety engineers, the latter part about software engineering managers. I know of no certification for any managerial level person (other than MBA programs, if you call that certification). There are such things as certified computer programmers, with specializations in areas like systems. I think the the CCP program is a useful one, although it perhaps does not go far enough, being based only on a test. Although I have a PhD in computer science, I took the CCP exam to see what it was like. I

passed, but I suspect many of my colleagues would not.
-mark

Response by Nancy: I obviously was unclear in my message. The Qualified System Engineer requirement is only for the person who assumes the responsibility for the system safety program (i.e., who acts as technical manager or technical lead), the other safety engineers are not required to satisfy the same requirements, and this person is certified as to technical ability, not management ability. It is similar to the certification as Professional Engineer -- very few engineers are so designated, but safety-critical and important projects often include the requirement for a Professional Engineer to be involved. The idea is to ensure that at least SOMEBODY is responsible and accountable that things are done right and there is somebody on the project with a chance of knowing HOW to do things right. I don't know anything about the CCP certification, but get the impression that it is a minimal qualification test rather than a process to identify the very best.

[I have grave doubts about some of the certification ideas -- and about the notion of system safety people, especially if done in the absence of intelligent system designs! PGN]

Search RISKS using swish-e

Report problems with the web pages to the maintainer

Search RISKS using swish-e

THE RISKS DIGEST

Forum on Risks to the Public in Computers and Related Systems

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

Volume 5: Issue 31

Friday, 21 August 1987

Contents

"Computer Failed to Warn Jet Crew"

Peter G. Neumann <Neumann@csl.sri.com>
Fri 21 Aug 87 08:34:09-PDT

The front page of the Washington Post this morning described the current hypotheses on the crash of the MD80, Northwest Flight 255, in Detroit on 17 August 1987. The flight recorder indicates that the flaps were not set for takeoff, although another Northwest pilot reported to the contrary. As most of you now know, the pilot and copilot apparently omitted the checklist procedure for setting the flaps. Today's addition to the emerging picture is that, when the attempted takeoff began, the computerized warning system failed to announce (by simulated voice) that they had neglected to set the flaps. It was supposed to. However, a subsequent computerized warning did indicate the final impending STALL, which indicates that the computer was at least working, contraindicating speculation that the warning system might

have failed because of the circuit breaker being turned off. This leaves open the possibilities of sensor failure, faulty wiring, and computer problems -- hardware failure, software misdesign, etc. (A flap indicator switch had failed on that plane in January and had been replaced, but this was apparently discounted in importance because of redundancy.) Another possibility being considered is that the flap and slat controls could have been properly set, but failed to deploy...

Risks to Privacy (re: RISKS 5.30)

Jerome H. Saltzer <Saltzer@ATHENA.MIT.EDU>
Thu, 20 Aug 87 10:14:37 EDT

Today's (Thursday, August 20, 1987,) Eastern Edition of the Wall Street Journal carries a page-one leader article on risks to privacy of government data banks and cross-agency record matching. Most of its material is likely to be familiar to RISKS readers, though it includes a couple of incidents I hadn't heard reported before.

Jerry

[Jerry pointed out western and eastern editions may differ.]

ATM features

Jack Holleran <Holleran@DOCKMASTER.ARPA>
Thu, 20 Aug 87 12:47 EDT

Reprinted from Readers Digest (page 111, August 1987) (without permission)

GUARD YOUR CARD

Many BANK CUSTOMERS do not realize that their automatic-teller machine (ATM) cards are not protected by the federal laws that cover credit cards like Visa and MasterCard (which have a $50 maximum liability if lost or stolen). ATM liability is also $50, but *only* if the card is reported missing within two days. After that, your liability rises to $500, and after 60 days the amount you could get stuck for is *unlimited*. So guard your ATM card and personal identification number (PIN), or you could lose a small fortune.

---Molly Sinclair in *Family Circle*

No wonder banks, etc. want us to have ATM cards.

Licensing software engineers

Frank Houston <houston@nrl-csr.arpa>
Thu, 20 Aug 87 10:10:21 edt

The following does not reflect my opinion on professional licensing, which I

believe mutually benefits both the licensee and the public, but reflects my concern about the amount of influence a license may carry.

While I am generally neutral about professional licensing, I am concerned about the practice of making a licensed individual "responsible" for safety, security or quality, just as I am concerned about assigning such "responsibility" to a specific department in any organization. Too often everyone in the company or project assumes that the "responsible" person or group will catch all problems; that the rest of the process can be a little sloppy, "..and besides there is a schedule to meet."

Of course the responsibles do not completely catch anything except the blame for what went wrong (which they try to shift to Murphy). Businessmen operate by the modern equivalent of the "Code of Hamurabi," but it is impractical to fire a whole engineering group or even a senior designer (expensive to replace); so the quality assurance department is the target of opportunity (low pay, low prestige). I'll wager that the average senior designer has twice the seniority of the average senior QA engineer.

The point that I am striving for is that assigning to SOMEBODY the responsibility for safety, quality or security, whether by licensing, title or regulation, is not only insufficient to solve the problem but may also be detrimental in the long run because it promotes complacency in the rest of the team.

In the quality assurance literature, anecdotes report that the most successful quality programs involve every person in the company, while the quality assurance department becomes more a scorekeeper that a line of error defense. The aphorism "quality is everybody's job" may be a cliche, but it holds much truth. I would say that quality, safety and security are everybody's jobs.

Everybody working on critical systems must consider himself/herself responsible for the quality, safety and security of the system; and until that sort of attitude takes root neither licensed engineers nor automated tools nor process standards will make the slightest dent in the risks we face.

Regarding the certification of software engineers

<benson%cs1.wsu.edu@RELAY.CS.NET>
Tue, 18 Aug 87 17:00:11 PDT

Nancy Leveson (<>)

<>Am I wrong in my observation that under-qualified people
<>are sometimes doing critical jobs and making important decisions?

Your observation appears correct to me.

<>Do you agree that some type of certification is necessary?

I would rather say that certification is highly desirable. Necessity is

a most difficult concept after one moves beyond the basics of air, water and food.

<>If so, there are still many open issues...

Yes, yes. But the basic issue is to obtain or create some certification agency. My attempt to interest the Society of Professional Engineers met with silence. My attempt to kindle some interest in this matter on RISKS about 15 months ago received no support, and at least one negative response. I conclude that it will take at least one major accident with significant loss of life, this accident attributable to software failure, before there will be sufficient interest to establish a certification program.

David B. Benson

Re: Risks of automating production

<mnetor!utzoo!henry@uunet.UU.NET>
Sat, 15 Aug 87 21:23:56 EDT

> From: Richard A. Cowan <COWAN@XX.LCS.MIT.EDU>
> ... In the end, I believe that
> automation will cause incredibly disruption and suffering unless there is
> also a dramatic shortening of the work week.

Much depends on what else is going on in the economy at the same time. By far the biggest example of technological unemployment in history (to date) is the mechanization of farming, which does not seem to have caused trouble on such a scale. This was relatively recent, too. As late as 1918, farming was so manpower-intensive that my grandfather missed combat service in WW1 because he (and thousands of others) got sent home on "harvest leave". I don't know what the numbers were like then, but over a longer time scale the percentage of farmers in the population has gone from >90% to <10%. Studying this enormous transition might tell us something about handling he advent of automation.

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

[At the rate we are going, by the year 2001 there will be more computer users than people (if you will pardon reuse of an old joke). But, no matter how many million programmers we have, the GOOD ones who are capable of disciplined work are always going to be at a premium. PGN]

Re: Automated environment control (RISKS 5.24)

Robert Stanley <roberts%cognos%math.waterloo.edu@RELAY.CS.NET>
20 Aug 87 00:21:40 GMT

In the early 1970's a (possibly apocryphal) story was doing the rounds. It concerned an installation of IBM's where the new physical plant had a

significant amount of its environmental controls in the hands of a computer. Unfortunately, a serious bug emerged during testing, which manifested itself by activating the fire-fighting system, which immediately powered down the systems (electronic equivalent of hitting the crash stop), eliminating all traces of the misbehaving software. After two repetitions the story reported that the project was abandoned.

I never troubled to track this one down, but it has stuck in the memory. The second story I can vouch for because I hired the senior system programmer shortly thereafter and he gave me the details. Unfortunately I am not at liberty to reveal the installation concerned, which probably invalidates this posting. [Not necessarily. We just have to take it for what it is. PGN]

A huge dedicated computer environment was constructed by one of the largest computer users in the UK. The main floor was so large, and the halon fire suppression on such a hair-trigger, that the operators had to practice gas-mask drills when the alarm sounded. By the same token, the exits were sufficiently distant that reaching them in a smoke/gas filled atmosphere could be a serious navigational problem. To help out, illuminated arrows were set into the floor panels, and a computer was supposed to light these to point the way to the nearest exit. Needless to say, this extremely costly system totally failed its first test because the primary control software shut down all systems, including the light control system, on detection of a fire/smoke problem.

I do not know how to cure this class of problem, which is akin to the self-powered emergency light for power failure. The reason for shutting down control systems in a fire emergency is obvious, but the idea of umpteen self-contained micro-processor-based emergency systems is equally horrifying. Imagine the software update problem, should the installation to be sufficiently advanced in its thinking to implement flexible response! By way of comparison, consider the Brown's Ferry near-disaster (We Almost Lost Detroit), where a fire in the (one and only) cable duct under the control room floor rapidly severed the control centre from everything over which the operators were supposed to have control. No matter that the fire started in an extremely bizarre fashion, the issue is how do you protect vital communication links in physically hazardous circumstances.

Robert Stanley Compuserve: 76174,3024 Cognos Incorporated
uucp: decvax!utzoo!dciem!nrcaer!cognos!roberts 3755 Riverside Drive
or ...nrcaer!uottawa!robs Ottawa, Ontario
Voice: (613) 738-1440 - Tuesdays only (don't ask) CANADA K1G 3N3

[For RISKS it's been halon cats and dogs lately; this one gets through. PGN]

Automated control stability and sabotage

<asci!brian@ucbvax.Berkeley.EDU>
13 Aug 87 11:56:51 PDT (Thu)

I write fiction on the side. Watching the discussion on automated control systems for such systems as air traffic control and power plants, I was reminded of a short story I wrote a few years ago that used a possible world

economic collapse as a plot device (though the theme was dramatically different). I've always been suspicious of Wall Street (the buying and selling of money for the sake of making money just strikes me as wrong, I think of investing as buying and staying). In my story I skirted the issue of how the collapse could be brought about, but intimated that someone wanted to do so by sabotaging a computer system somewhere. Recently I've been thinking such a collapse is now possible by the deliberate sabotage of a computer system used by brokerage houses.

As I understand it, these systems watch the difference in say the price of company A and a bond from company B. When the price of the bond becomes attractive for reasons I don't understand, the computer starts dumping hundreds of thousands of shares in company A and buying in company B. Another computer sees the drop in company A and starts selling to cut its losses. Another computer and watches the drop, and starts buying in A when it thinks it is a good value. TIME had an issue about the electronic market and talked about a program called Firedown that did something like this.

> [And RISKS has had considerable discussion in past volumes on instabilities that can result from closed-loop computer models. PGN]

My question is what if somebody sabotaged such a system or group of systems, and they started selling everything and bought into say gold. Is there a risk that an "electronic" panic could be started with all of these machines selling and selling, generating an avalanche effect? It seems from media reports that the speed of the buying and selling transpires much too fast for human intervention, and the programs are DESIGNED to work without human intervention. What prevents such an occurrence? If sabotage is possible, and an avalanche could be generated, what precautions could be made to stop it (maybe a government computer monitoring the whole thing that steps in and starts buying everything up to slow and eventually stop the avalanche, later it starts an organized sell of everything it bought)?

With what appears to be agreement that fully automated control systems have enormous dangers and that human intervention is demanded, what about these Wall Street beasts? I don't know, but as a writer I'm very curious what others might know.

Brian Douglass, Applied Systems Consultants, Inc. (ASCI), P.O. Box 13301,
Las Vegas, NV 89103 Office: (702) 733-6761 Home: (702) 871-8182
UUCP: {mirror,sdcrdcf}!otto!jimi!asci!brian

> [Certain safeguards are clearly desirable, both preventative and real-time monitoring. But we learn from such situations that it is essentially impossible to anticipate every possible instability mode. The ARPANET collapse of 1979 was an example of a seemingly impossible event happening. PGN]

Trusting Computers (Re: RISKS 5.27)

ihnp4!illusion!marcus@ucbvax.Berkeley.EDU <Marcus Hall>
Fri Aug 14 08:14:53 1987

> Her ... cash card had been used to steal 250 pounds (the daily limit ...
>
> Elsewhere, Abbey National claims to process 5.7M transactions per year ...

> The moral is: don't expect computers to perform all the routine,
>boring tasks that they do so much better than people.
>
> Andy Walker, Maths Dept, Nottm Univ, UK

No, the problem just has to be looked at differently. To enforce the 250 pound per day limit, the computer has to have fields in its customer records that indicate the date of the last withdrawal and how much has been withdrawn on that date so far (or some such information). To enforce the "3 consecutive day" rule, merely add another two bit field that indicates how many consecutive days the account has hit the max withdrawal limit. Of course, the easy way around this is to withdraw 249 pounds per day, so this probably isn't what you want to be looking for, but the scheme can be adapted to many different trigger conditions.

The moral here is: Don't be blinded into believing that the obvious solution is the only solution.

I wounder how much computing power is wasted in the world because poor algorithms are implemented and give acceptable enough performance to just get by?

Marcus Hall

Search RISKS using swish-e

Report problems with the web pages to the maintainer

Search RISKS using swish-e

THE RISKS DIGEST

Forum on Risks to the Public in Computers and Related Systems

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

Volume 5: Issue 32

Friday, 4 September 1987

Contents

Honda eschews computers for new 4-wheel steering system

Roy Smith <cmcl2!phri!roy@seismo.CSS.GOV>
24 Aug 87 02:03:54 GMT

In the September SciAm, there is an ad from Honda announcing that the new Prelude Si4WS has 4-wheel steering. I seem to remember this type of steering being discussed at some length on this list in the past, so I won't go into the details other than to quote the following from the ad:

"The rear wheels are linked directly to the front wheels by a steering shaft, gears and rods. There are no computers, wiring or electronic black boxes. The Honda system is mechanical and sure."

Have the Honda engineers been reading RISKS, I wonder? Perhaps our discussions steered them away from electo-gadgetry? Has car design turned a corner because of us?

Roy Smith, {allegra,cmcl2,philabs}!phri!roy
System Administrator, Public Health Research Institute
455 First Avenue, New York, NY 10016

Another Trojan Horse?

Brian Tompsett <mcvax!ecsvax.ed.ac.uk!BCT@seismo.CSS.GOV>
24 Aug 87 15:39:48 BST

The following is quoted the Engineering Computing Newsletter of the Rutherford Appleton Laboratory, Issue 4:July/Oct 87. The article describes a visual version of the file comparator program diff called vdiff.

"Recently, the staff of the Houses of Parliament have become interested in this work, since they need to monitor changes to Bills as they pass through Parliament. As a result, we are planning a new feature whereby vdiff secretly adds extra lines to a file without the user knowing. Our future funding may therefore come from an extra clause in an Act of Parliament, supporting us in perpetuity at a base in Tahiti with ..... . "

Brian Tompsett. Department of Computer Science, University of Edinburgh,
JCMB, The King's Buildings, Mayfield Road, EDINBURGH, EH9 3JZ, Scotland, U.K.
Telephone: +44 31 667 1081 x3332.
JANET: bct@uk.ac.ed.ecsvax ARPA: bct%ecsvax.ed.ac.uk@cs.ucl.ac.uk
USENET: bct@ecsvax.ed.ac.uk UUCP: ...!seismo!mcvax!ukc!ecsvax.ed.ac.uk!bct
BITNET: psuvax1!ecsvax.ed.ac.uk!bct or bct%ecsvax.ed.ac.uk@earn.rl.ac.uk

Transatlantic Flights at Risk from Computer

Daniel Karrenberg <mcvax!cwi.nl!dfk@seismo.CSS.GOV>
Wed, 26 Aug 87 01:40:37 +0100

The obvious mistakes being made here are well known to Risks readers:

1) no backup systems or backup copies of vital real-time information,
2) discrediting anonymous reporting schemes.

Daniel Karrenberg, Centrum voor Wiskunde en Informatica, Amsterdam
Phone +31 20 5924112 Future Net: <dfk@cwi.nl>

[But the following is worth including anyway. Who do you know who never makes obvious mistakes? PGN]

From "The Independent" of August 24th:

Transatlantic flights at risk from computer, By David Black

The computer which controls airliners flying between Europe and North America failed yesterday morning, causing delays of up to three hours on all transatlantic flights.

It is the ninth serious breakdown of the system, which has had, on average, minor failures every other day since it became operational earlier this year.

It crashed just after 11.30am. By mid-afternoon Heathrow airport began to run out of parking space for delayed aircraft, many with passengers on board. Similar delays were experienced at Paris, Schipol (Amsterdam), Frankfurt, Zurich and other major European airports and complaints from airlines began flooding in last night. The failure on the busiest day of the year is bound to embarrass the Civil Aviation Authority internationally.

Although the computer was restored by tea time, controllers were unable to bring it back on line without stopping all transatlantic traffic. Last night, the intention was to wait until traffic eased prior to the surge of eastbound traffic from North America before restoring the computer.

The computer, known as the Flight Data Processing System (FDPS), is based at the National Air Traffic Service's Oceanic centre at Prestwick in Scotland. Yesterday's failure is the second in which all information available to controllers was wiped from the system.

Controllers there monitor weather systems over the Atlantic and every day draw up a network of airways, known as the Organized Track Routing system, offering the quickest transit times. So busy was demand yesterday, that instead of six parallel tracks, nine were planned.

The computer takes data from domestic air traffic control centres and works out the times at which aircraft will enter Oceanic airspace. Safety for aircraft crossing the Atlantic depends entirely on separation, not by radar, but by releasing the planes into the track system at regular intervals.

All movements are displayed on large screens which yesterday had to be isolated from the computer, with flight details entered manually. Strict flow control limiting the number of airliners allowed to enter the tracks was then imposed to prevent collisions.

The new system is all electronic, and when the screens go blank, there are no printed cardboard progress strips to fall back on. It is the subject of highly critical reports in the latest CHIRP (Confidential Human Factors Incident Reports) bulletin, which is published by the RAF's Institute for Aviation Medicine. CHIRP allows pilots and controllers to report incidents in confidence, without jeopardising their or their colleagues' careers while alerting others in the aviation industry to possible safety problems.

It is based on a similar scheme in the US, run by NASA. However, last week, in advance of publication of the latest CHIRP bulletin, the CAA said that because references which could identify staff were removed, the reports lacked sufficient detail to be investigated, and were undermining flight safety.

One controller used that CHIRP bulletin to describe what happens during a system crash: "On one occasion when the system crashed all information available electronically to staff was wiped out. For two and a half hours the staff had no idea what traffic was in their area."

The oceanic controllers were reduced to telephoning adjacent air traffic control centres to find out which airliners had been handed over to the recently, and to examining old strips to get some kind of picture what airliners were flying, supposedly under their control.

Adjoining control centres, meanwhile, had to hold airliners on the boundary between their area and Oceanic's while the mess was resolved.

During one crash, a westbound and an eastbound airliner were accidently placed on a collision course 35,000 feet over the Atlantic. The controller concerned wrote: "The potentially horrific situation was resolved by pure good luck when another controller noticed that the eastbound was missing from the display, and may have been deleted by mistake."

A senior controller at the Oceanic centre said last night:
"They wonder why we have so little confidence in our top management when they give us tools like this - aeroplanes have to have duplicated or even triplicated systems as back-up, but the same safety rules clearly do not apply to our equipment. These continual failures are the basic ingredients of a mid-air disaster."

Christopher Tugendhat, the chairman of the CAA, was unavailable for comment yesterday.

Re: "Computer Failed to Warn Jet Crew" (RISKS DIGEST 5.31)

<sdcsvax!ames!hoptoad!academ!killer!era@ucbvax.Berkeley.EDU>
Mon, 24 Aug 87 03:19:50 CDT

With regard to the crash of Northwest Flight 255, if the faulty fasteners that are common throughout military and nuclear installations have also been used in civilian aircraft, it is not entirely impossible that the flaps deployed but broke off the moment stress was applied in takeoff. These bolts do not meet design specifications, and are not ordinarily detected by maintenance workers.

--Mark Ethan Smith

[Incidentally, Danny Cohen noted that my implicit assumption that the flap warning system might have been working because the stall warning system was working was unjustified -- the two systems are independent. "In the MD-80 there are 2 independent Stall Warning Systems, one of which shares a power supply with the Takeoff Configuration Warning System (TCWS) that is supposed to warn about incorrect flap setting on takeoff." But the common power supply does indeed imply that the circuit breaker did not fail. Furthermore, it now appears that the flaps WERE retracted (not deployed) on takeoff, in spite of the visual testimonies of other pilots, and that would make it very hard to take off. PGN]

Delta-Continental Near-Miss

Peter G. Neumann <Neumann@csl.sri.com>
Fri 4 Sep 87 13:24:57-PDT

The 4 Sept 87 papers note that the Delta L-1011 flight on 8 July 1987 that was 60 miles off course actually came within 30 feet of colliding with the Continental 747, and that four of the five safety measures that had been previously recommended had been ignored, including plotting the expected course on a map -- in fact, the appropriate chart was not even on board. The cause of the near-miss is attributed to false data entry of the inertial navigation heading. Both the USA and Canada announced stepped-up use of redundant checks in the navigational procedures...

Decomposing Software

<hplabs!intelca!ceg@ucbvax.Berkeley.EDU>
Fri, 21 Aug 87 17:30:31 PDT

The other day I was called in to repair an old terminal which was spewing random characters across the screen. I tracked the problem down to the keyboard, specifically the i8741 microcontroller. (BTW, the i8741 is an 8 bit intel uController with 1k EPROM & 64 bytes RAM) This uController and the keyboard had manufacture dates of early 1977. I was in school in 1977, and the EPROM cells were touted as being able to store a charge for 10 years (nearly infinite time for systems where time is measured in nanoseconds :-)), so no one ever cared about 10 years in the future. Guess what? It's now 1987 and in comparing the EPROM code with another device, some entire words had floated to back to FF, causing the failure. I was thinking about how many other computer keyboards/systems had older style EPROMs and how the firmware was slowly decomposing. Where might these controllers be? ICBM launch control systems? ATM machines? Pacemakers? Now I have something else to lay awake at night and worry about. :-)

Charles Gard

Why the Phalanx Didn't Fire (IEEE Spectrum Reference)

Eugene Miya N. <eugene@ames-pioneer.arpa>
Thu, 3 Sep 87 17:02:30 pdt

%A John A. Adam
%T USS Stark: What Really Happened?
%J Spectrum
%V 24
%N 9
%D September 1987
%X Cover "Why the Phalanx Didn't Fire"

Cheap modems and other delights (Compuscan warning)

<ihnp4!inuxc!iuvax!iucs!bobmon@UCBVAX.BERKELEY.EDU>
Friday, 14 August 1987 14:21-MDT

I recently posted a request for info about a company offering a modem for $122 (at least two other people posted similar queries). I've since seen the following bulletin, which I am passing along...

Message #1951
To ALL 08-11-87
>From STEVE LEON (SYSOP) Subject WARNING

There is an ad appearing in BYTE, INFO WORLD, Compuserve's ONLINE and perhaps other places (it may be scheduled for PC WORLD). It is a full page ad by an outfit in Beverly Hills California called Compuscan. Prices are absurdly low - in fact - they are below wholesale.
To make a long story short - the whole thing is a scam. We have the postal authorities on it. INFO WORLD will have a front page story next week on it.
In the meantime, don't fall for it. If you already have - RUN to the bank and stop payment on the check. (Get to the bank in person and get it from them in writing that you told them.) If you already sent money and your check was cashed - next time remember the old -but true fact - that if sounds too good to be true - chances are it is not true.
Please pass it on through the BBS networks.
STEVE LEON

Reach out, touch someone

Michael Sclafani <sclafani+@andrew.cmu.edu>
Fri, 28 Aug 87 17:57:57 edt

From The Miami Herald, August 14, 1987.

It's 10 p.m. Do you know where your children are? No? Well, just dial them up on your computer, via satellite link to the tiny implant embedded just behind their left ears.

This is not science fiction. Dr. Daniel Man, a Boca Raton plastic surgeon, just won a patent on the basic technology.

He says the satellite link won't work until he perfects techniques for making the human body act as an antenna. Be he predicts its use by parents, pet owners, overseas workers in potential hostage situations, Alzheimers's patients and police tracking criminals or parolees.

Does Dr. Man see any hint of Big Brother in all of this?

"Yes, but I don't want to go into it. I'm more into the technical

aspects."

[What will it take before inventors of technology consider implications of their work as part of their responsibilities? MS]

SDI event (Physicians for Social Responsibility)

Gary Chapman <chapman@russell.stanford.edu>
Tue, 25 Aug 87 11:52:43 pdt

"AN UPDATE ON THE STRATEGIC DEFENSE INITIATIVE"

September 15, 1987
7:30 p.m.
Stanford University
Dinkelspiel Auditorium
Admission is free

Sponsored by the Stanford/Mid-Peninsula Chapter
Physicians for Social Responsibility

Panelists:

David Redell -- DEC Systems Research Center, Palo Alto, CA

Gary Chapman -- Executive Director, Computer Professionals for Social Responsibility, Palo Alto, CA

Professor Joseph Goodman -- Department of Electrical Engineering, Stanford University

Angelo Codevilla -- Research Associate, Hoover Institute, Stanford, CA

The panel will be moderated by Dr. David Bernstein, of the Stanford Center for International Security and Arms Control.

This panel discussion is intended to review the current state of the Strategic Defense Initiative in technical, political and research terms. There will be a period for questions and answers after the panelists speak, which is scheduled to take about 80 minutes.

Dinkelspiel Auditorium is directly in front of Tressider Student Union of Stanford, on the west side of the campus.

Report problems with the web pages to the maintainer

Search RISKS using swish-e

THE RISKS DIGEST

Forum on Risks to the Public in Computers and Related Systems

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

Volume 5: Issue 33

Friday, 4 September 1987

Contents

How to Beat the Spanish telephone system

"Lindsay F. Marshall" <lindsay%kelpie.newcastle.ac.uk@Cs.Ucl.AC.UK>
Tue, 1 Sep 87 11:35:00 BST

SPANIARDS LEARN THE PRICE (ART) OF PHONE PIRACY (From the Independent)

Madrid -- The ears of officials at the Spanish telephone company Telefonica, are burning at an article printed in a Dutch newspaper that ran instructions on how anyone with a computer hooked up to their telephone can dial around the world at Telefonica's expense.

Such telephone piracy has plagued other countries, such as the United States, Britain and Germany who were forced to end this electronic joy-riding.

But according to the Dutch Newspaper, Volksrant, Spain, Portugal and Italy all lack the means of tracking down pirates who ride the 'bridges' -- those who ring anywhere in the world, and talk as long as they want, courtesy of the intermediate or 'bridge' method.

The method is like an electronic shell game, whereby the pirate calls a busy number in Spain through his local operator. Then using that open line to Spain, the pirate coaxes(!@??) the right series of sonic signals through his computer to ring elsewhere at the telephone company's cost.

A Telefonica spokesman said that the number of callers hitching free rides on the Spanish system is 'infinitesimal'. But he said most European telephone companies had a gentleman's (?sexist) agreement to split the costs incurred by the pirates.

rosa

Re: Automated control stability and sabotage

Amos Shapir <nsc!nsta!nsta.UUCP!amos@Sun.COM>
22 Aug 87 19:33:35 GMT

[... about affecting the values of shares by sabotaging computers]

Actually something like this was attempted here lately - someone called a broker, posed as a customer and placed huge purchasing order for a certain share; luckily the purchasing bank's computer flagged the order as suspicious and it was never carried out. This time the fraud was done by a human, and the computer caught it. I guess Wall Street computers may be protected much better.

Amos Shapir, National Semiconductor (Israel)
6 Maskit st. P.O.B. 3007, Herzlia 46104, Israel Tel. +972 52 522261
amos%nsta@nsc.com (soon to be amos%taux01@nsc.com) 34 48 E / 32 10 N

Crisis in the Service Bay (condensed from Toronto Star)

Mark Brader <msb@sq.com>
Tue, 1 Sep 87 12:33:43 EDT

The evolution of the species -- from grease monkey to service technician -- is behind schedule. Our education, apprenticeship, and retraining system is not keeping pace with the spread of electronics and new high-tech components through cars, say service experts. They point to a crisis ...

Improvements in quality and defect avoidance have spared most new car owners the worst effects of a repair industry that's technically dated and starved for able new recruits. But watch out when today's cars and those of tomorrow start wearing out.

Already some consumers are enduring multiple visits to dealerships to cure

such aggravations as stalling, quitting, rough idling, hesitation, and odd noises, not to mention more serious problems. ...

Each year, literally millions of dollars worth of computer controls are being removed from cars unnecessarily when mechanics can't trace the true source of problems. ...

Today's average mechanic in Canada is in his [sic] mid-30's. He completed his training more than a decade ago, before computer controlled emission and engine management systems, anti-lock brakes, or widespread use of turbochargers. Add to that the coming electronically controlled four-wheel driving and four-wheel steering systems.

"There is nothing in the auto mechanic program that says you have to go back to school for upgrading", says [Ford of Canada's William] Rowley. "Most fellows have been out of school so long, they don't know how to learn any longer."

Rowley says there's also a problem with the compensation system for mechanics. A fellow can often earn more doing routine service tasks, like brake repairs, than he can earn puzzling over a mysterious electronic problem. ...

Rowley believes every new-car dealership should have one electronics specialist by 1990 and half of new-car mechanics should have these skills by 1995. ...

James Lanthier, ... [of] Ontario's Ministry of Labour, says 598 Ontario mechanics are now spending weekends completing three trade updating courses. None has yet finished more than the first course, which began in January, on the fundamentals of computerized vehicle management systems. And these students are only a minority of the 15,000 mechanics in Ontario involved directly in repairing cars. ...

Ford's Rowley complains ... that community [i.e. vocational] colleges are still graduating apprentice mechanics who have not been exposed to some of the latest technical features of cars. He says most college curriculums are three years out of date. ...

Only recently has the auto industry persuaded the federal government to take a leadership role in trying to help provincial education authorities set a course of action. ... If any provinces took immediate action ... the first of a new crop of high-tech auto technicians would be collecting their licenses some time in late 1993. And even that may be too optimistic.

Condensed by Mark Brader from a column by James Daw that appeared in the Toronto Star on August 29, 1987.

Who is responsible for safety?

Nancy Leveson <nancy%murphy.uci.edu@ROME.UCI.EDU>
Fri, 21 Aug 87 13:27:29 -0700

>From Frank Houston (Risks 5.31):
>The point that I am striving for is that assigning to SOMEBODY the
>responsibility for safety, quality or security, ...

While it is obvious that safety or security or any other important software quality must be the concern of everybody or it will not be achieved, that does not mean that assigning responsibility is not necessary nor that everybody (en masse) can perform the necessary activities to achieve it. One of the main reasons for the growth of the system safety engineering field is that the early missile systems were so unsafe. The basic procedure for achieving safety in these early systems was to assign responsibility for safety to everybody. Unfortunately, there are always conflicting goals in any engineering design process. These goals need to be prioritized and decisions made with respect to these priorities and with knowledge about how the decisions will affect the ultimate quality goals of the entire system under construction. The responsibility for setting goals and priorities rests with management. But to then assign responsibility to every engineer and designer to make all decisions about conflicting goals means that each person must understand all the implications of every decision they make on every part of the larger system under construction. This is unrealistic because for any reasonably complex system, each person cannot possibly have all the information necessary to make these decisions.

The individual engineer is responsible for implementing the safety requirements for the component or subsystem under his control. But there needs to be a systems safety engineer who is responsible for deriving those individual subsystem safety requirements from the SYSTEM safety requirements, ensuring that the design personnel are aware of them (so that they can implement them), providing the interface point for questions that arise as the design progresses (requirements on any real project are not completely specified before design begins and never changed thereafter -- for one thing, the design process itself suggests additional requirements), etc. My personal belief after studying complex and large projects is that there is a necessity for a software safety engineer to interface with the system safety engineer. The reason for the extra level of interface is the complexity of the software subsystem and the practical problems of training a person to be an expert in all aspects of engineering and computer science. The software safety engineer is responsible for performing the duties listed above for the system safety engineer but with respect to the software subsystem and for interfacing with the system safety engineering group which is dealing with the larger questions of the interfacing between the subsystems. This does NOT imply that each person is not responsible for the quality of the subsystem on which they are working, only that they cannot possibly be responsible for understanding all aspects of the entire system and that decisions about such things as safety and security cannot be made individually and in a vacuum by hundreds of people without any central coordination or planning function.

So yes, safety must be designed into the system by each individual on the project. But somebody must provide them with the information necessary to do that. And that person (or group) has the responsibility for the correctness of that information and for getting that information to the people who need it in a form and at a level of detail that can be most effectively used by those people.

Nancy Leveson, University of California, Irvine

Certification of Software Engineers

Brian Tompsett <mcvax!ecsvax.ed.ac.uk!BCT@seismo.CSS.GOV>
24 Aug 87 11:38:21 BST

Just a brief contribution to the debate on the Certification of Software Engineers. In the UK Software Engineers may apply to be recognised as a "Chartered Engineer", by the Engineering Council. This gives the software engineer the same status/rights as a chartered civil or nuclear engineer.

The applicants qualifications and experience are examined by an admitting body to ensure that he meets the required standard. The British Computer Society is in the process of nominating members to Chartered Engineer Status. Membership of the BCS requires sufficient academic or relevent commercial experience and the member has to adhere to a code of professional conduct.

In the UK, therefore, there is a growing body of certified and experienced Computer Professionals recognised by their peers, who are qualified to undertake work to the standards required.

Brian Tompsett, MBCS.

Brian Tompsett. Department of Computer Science, University of Edinburgh, JCMB, The King's Buildings, Mayfield Road, EDINBURGH, EH9 3JZ, Scotland, U.K.
Telephone: +44 31 667 1081 x3332.
JANET: bct@uk.ac.ed.ecsvax ARPA: bct%ecsvax.ed.ac.uk@cs.ucl.ac.uk
USENET: bct@ecsvax.ed.ac.uk UUCP: ...!seismo!mcvax!ukc!ecsvax.ed.ac.uk!bct
BITNET: psuvax1!ecsvax.ed.ac.uk!bct or bct%ecsvax.ed.ac.uk@earn.rl.ac.uk

---

Certification (Re: RISKS 5.28)

Richard Neitzel <udenva!rneitzel@seismo.CSS.GOV>
Wed, 26 Aug 87 19:14:03 mdt

A Firm NO to certification. Richard Neitzel, Rockwell International, Golden, CO

In her recent article Nancy Leveson states:

> ...Am I wrong in my observation that under-qualified
>people are sometimes doing critical jobs and making important decisions?

No, you are not wrong in your observation, as many under-qualified people are working out there. However, I seriously doubt that any system of proscribed training, education, experience, etc. will be either effective or of use to much of the computer industry. I will base this on three observations.

First, there is the implicit assumption that engineers are particularly intellegent and able persons. Having worked with engineers from all sorts of backgrounds, and being one myself, I honestly feel that the number of under-qualified, and in some cases, out right ignorant, engineers

is staggering. This applies equally to persons with years of "experience" as to recent graduates. I have worked with "recognized experts" who obviously knew little more about their subject then I.

Secondly, and closely related to the first item, is the assumption that by using tests, experience criteria, etc. we can determine whom are qualified persons. As a former certified nondestructive testing Level II, I can testify from personal experience that such programs have severe problems. For those not familar, nondestructive testing is a highly specialized field that invokes the inspection of items for defects using such methods as ultrasonics, radiography, and eddy currents. Since one missed defect could cause a disaster, such as an airline crash, the need for qualified persons is obvious. Under the agency of the American Society for Nondestructive Testing, a program of training, testing and certification has been in use for over 20 years. Unfortunately, it has not proved adequate to the task. First, given human nature, fraud has been a part of the system. By requiring certification, the number of available people is cut sharply. This means that the incentive for both employer and employee is great to falsify certifications. Second, the program has proved to have only a small bearing on the quality of the persons who are certified. Recent studies have shown that only 60-70 percent of the persons certified are performing at an adequate level and out of those most are only performing their jobs at the 70th percent level.

Third, who will determine what the standards are to be? Is it truly possible for a committee to determine what is suitable for a board spectrum of industries? Drawing again on my NDT experiences, it has been discovered that persons who are excellent in testing nuclear power plants have no luck in aircraft inspection and vice versa. The blanket certification fails because it must be too general, in order to cover the entire field. The result has been that industries are requiring additional testing, etc. for their own areas. Once this starts to occur the attempt to quanitify someones ability in an area outside of the one in which they are currently working is impossible. Do we really want to limit job mobility this way?

For these reasons I am against attempting to overly regulate who may call himself a "software engineer". I should like to close with two parting thoughts:

1> Some of the most creative and effective programmers I have ever worked with had no formal CS training (one dropped out of college after 2 years and the other is a philosophy major). Conversely, one of the worst was a bona fide CS graduate with 2 years experience, whose code was simply a wooden copy of the "proper" way to program.

2> Medical doctors, who frequently make life or death decisions, are required to pass their board exams only once (the same is true of lawyers). Thereafter, they are judged only by the quality of their work. Isn't that exactly what we are doing now?

The opinions expressed are mine alone and do not reflect any position on this issue by Rockwell.

Re: Regarding the certification of software engineers

Wilson H. Bent <allegra!vax135!whb@EDDIE.MIT.EDU>
Wed, 2 Sep 87 15:03:17 EDT

>From: <benson%cs1.wsu.edu@RELAY.CS.NET> (David B. Benson)
> I conclude that it will take at least one major accident with significant
> loss of life, this accident attributable to software failure, before there
> will be sufficient interest to establish a certification program.

But this is the trouble with software certification, with Star Wars testability, with software copyright protection, with Look-and-Feel lawsuits, etc, etc: the slipperiness of software.

For each of the cases presented in RISKS recently (ATMs and other bank errors, air and rail traffic control, power station control), I can see a long and drawn-out legal battle over accountability and responsibility. Who, for example, would be held responsible for improperly programming the flap controllers and monitors responsible for the recent Detroit air crash? Assuming that one person or group were found responsible, would they be personally liable, or the company? Consider the Morton-Thiokol hearings: a fairly clear case of a bad product, and a lot of finger-pointing. Where did the blame finally rest?

My point is: Yes, if there were such an accident which was clearly the result of software failure, it *might* lead to a certification program. Unfortunately, I don't envision such an accident, or rather such an assignment of guilt.

Wilson H. Bent, Jr. ... ihnp4!hoh-2!whb
AT&T - Bell Laboratories (201) 949-1277
Disclaimer: My company has not authorized me to issue a disclaimer.

Irish Tax Swindle

J.JXM@HAMLET.STANFORD.EDU <John Murray>
Fri 28 Aug 87 19:04:14-PDT

The Aug 14 1987 issue of "The Phoenix", an Irish investigative magazine, tells of a tax swindle currently being investigated there. The taxation authorities are the Revenue Commissioners (abbrev. Rev Comm) and the Collector General (abbrev. Coll Gen). Checks paying tax bills and using the abbreviations as payee were misappropriated by crooked tax officials, who altered the payees to "Trevor Commerford" or "Collette Gerald". Accounts in these bogus names were opened all over Dublin. Flaws in the offices' (manual) procedures allowed the crooked officials to effectively 'lose' the defaulter's files in the bureaucratic system. The defaulter is typically happy never to hear from the tax office again, even though s/he may only have paid a portion of the bill.

"A crucial factor in the whole fiddle is the modern banking
practice of retaining checks and noting only the amount debited

on customers' accounts. In days gone by, alterations to the payee line would have been immediately obvious to the payer when the check made its way back with the routine statement."

While writing this, I've thought of two other stories related to Irish banks. One involved using dud checks to earn interest during a prolonged bank officers' strike. The other concerned a microcode fix I applied to the Bank of Ireland system which stopped it dead overnight, with an apparent "loss" of several million pounds.

John Murray

Pogo Wins a Free Lunch -- Costs and Liability in Good Systems

"guthery%asc@sdr.slb.com" <GUTHERY%ASC%sdr.slb.com@RELAY.CS.NET>
Thu, 27 Aug 87 08:20 EDT

Does building a high quality, safe, reliable, and secure instance of a system cost more than building a low quality, unsafe, unreliable, and insecure instance of the same system? If not, then the safe one, being of equal cost, will surely out sell the unsafe one and the folks who build the safe one will prosper and those who build the unsafe one will not. Notwithstanding catchy phrases, generally speaking, quality, safety, reliability, and security are not free. Who then absorbs their cost?

Frank Houston proposes that the builders themselves absorb the additional cost when he suggests that "quality, safety and security are everybody's jobs." As the Japanese and Korean experiences have taught us, this works. The Japanese auto worker does more work for a given amount of money than an American worker. Japanese cars cost the same as American cars, you get more for your money with Japanese cars, and the builders of Japanese cars prosper and the builders of American cars do not.

Will this approach work with software and computer systems? Enterprise A pays 10 engineers $50,000/year each and builds Product A. Enterprise B pays 15 engineers $33,333/year each and builds Product B which costs the same as Product A but is of higher quality, safer, more reliable, and more secure. My expectation is that there will be a net flow of engineers from Enterprise B to Enterprise A. Why?

I don't know but I can think of a possibility. The amount of the cost of quality, safety, reliability, and security that computer system engineers are willing to absorb is not perceived by them to be sufficient to make a difference in the system's customer's buying behavior. Thus, Product A will sell just as well as Product B but A's engineers will do much better than B's engineers. Thus, I don't think the Japanese approach will work with computer systems.

The only alternative is that the system's customer absorbs the additional cost. What are computer system buyers willing to pay for quality, safety, reliabity, and security? The marketplace evidence says to me that without any downside risk for their absence, damn little. Thus, as long as we are willing to accept the excuse that the computer malfunctioned and no one is

to blame then we can't be expected to be asked to build high quality, safe, reliable and secure systems.

MORAL: If you want build good systems then you either have to be willing to absorb more of the cost of doing so or be willing to accept liability for not doing so. If you are willing to do neither, then you should expect to only build low quality, unsafe, unreliable, and insecure systems ... and that's just what we're doing. "We have met the enemy and he is us." Pogo

---

Re: Bank Computers and flagging

<bfisher.ES@Xerox.COM>
21 Aug 87 16:31:42 PDT (Friday)

Joe Herman's account was most interesting, especially in re the ATM not reflecting the true balance. I withdrew some bucks via an ATM on a Friday - and a few days later, Tuesday - had occasion to withdraw some more. The receipt after Tuesday's withdrawal showed a balance significantly higher than the amount prior to Friday's transaction. I double checked and found no EFT or normal deposits outstanding. I called the hot line and was told that I probably had transacted during a "float adjustment" period and that the amount indicated on Tuesday's receipt was not actually there. I was then informed that if I had transacted a few minutes later the receipt probably would have indicated the "real" amount. A couple of other minor incidents similar to this have convinced me that I must be going right down the rabbit hole every time I enter a bank parking lot. I don't remember signing an agreement that they could fiddle with my account for adjusting anything.

Bill Fisher

Search RISKS using swish-e

THE RISKS DIGEST

Forum on Risks to the Public in Computers and Related Systems

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

Volume 5: Issue 34

Monday, 7 September 1987

Contents

Dutch Police Hampered By Faulty Computer System

Patrick van Kleef <mcvax!cs.vu.nl!kleef@seismo.CSS.GOV>
5 Sep 87 16:49:11 GMT

Criminals are set free, innocent people get arrested due to serious problems with the central computer of the Dutch police. The newly installed computer at the CRI (Central Investigation Information dpt.) in The Hague, Holland, is invested with bugs. Police departments all over Holland have decided not to use the CRI computer anymore, until the problems are solved.

Only one day after the computer was installed, problems started occurring, giving inaccurate or plain incorrect information about people the police wanted to check. Innocent people appeared to be on a 'wanted list', criminals were 'cleared'. This resulted in injust arrests or people sent away whereas they should have been arrested. The chaos was enormous.

The CRI clearly made the blunt mistake to completely dispose of the old system and switching to the new system at once. No back-up system was maintained. And the supplier of the software ("It's not our fault, we've delivered what was ordered") washed his hands in innocence, blaming the police for incorrect usage of the system.

Will they never learn?

Paul Molenaar, freelance journalist

Computer Psychosis

Bill McGarry <decvax!bunker!wtm@ucbvax.Berkeley.EDU>
Fri, 4 Sep 87 22:38:41 EDT

United Press International [4 Sep 87]

COPENHAGEN, Denmark -- A young man became so mesmerized by his computer that he was hospitalized with a "computer syndrome" that made him unable to distinguish between the real world and computer programs, a Denmark medical journal said.

The journal said the unidentified 18-year-old contracted the new form of psychosis, called computer syndrome by three doctors at Copenhagen's Nordvang Hospital, after spending 12 to 16 hours a day in front of his computer.

The doctors said the young man began to think in programming language, waking up in the middle of the night thinking, "Line 10, go to the bathroom; Line 11 next."

The patient told the doctors he "discovered that man is only a machine. There is no difference between the computer and man."

In WEEKLY FOR PHYSICIANS, psychologist Bent Brok and psychiatrists Eva Jensen and Erik Simonsen said, "He merged with the computer and afforded it supernatural qualities."

In the end, he suffered from insomnia and anxiety and had to be hospitalized. The article did not indicate his present condition.

The young man's preoccupation with computers is not unique, but his psychotic condition is unusual, Tuesday's report said, warning against "many young people's excessive preoccupation with computers."

The three doctors said that the computer is used by youths as a substitute for human contact because it always responds in a rational manner but that the stress on logic can lead to immaturity and emotional limitations.

The computer trade itself also seems to be aware of the problem.

"A large group of young people -- about 95 percent of them boys -- are computer freaks who live for nothing but the machine," said Lars Knudsen, 32, manager of a Copenhagen computer firm, Professional Datainformation.

"The typical computer freak is between 14 and 16," said Knudsen, a former freak himself. "He gets up at 2 in the afternoon and sits in front of the screen until 4 in the morning. He drinks 3 liters of Coke and has no girlfriend."

Risks and people

Alan Wexelblat <wex@MCC.COM>
Sun, 6 Sep 87 13:42:20 CDT

Two short notes:

> The "were the flaps extended" debate has made me remember just how unreliable human eyewitnesses are. Many times we depend on human observation to back up sensor data. Yet we forget about the people who "saw" the plane on fire before it hit the ground, and the pilot of the plane behind who "saw" that the flaps were extended.
>
> The comments by Rich Neitzel about certification have also reminded me of the risks of natural language. At one point in his "NO to certification" message, Neitzel uses "proscribed training" where he means "prescribed training." Of course, this totally reverses the meaning. It is not hard to imagine such an error being written into the specification for a system, leading to behavior totally opposite that which was desired.

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

The influence of RISKS on car design?

<COHEN@C.ISI.EDU>
4 Sep 1987 17:43:51 PDT

Roy Smith (System Administrator, Public Health Research Institute, NYC) remarks (in RISKS DIGEST 5.32) about Honda's 4WS (4-wheel steering) having "no computers, wiring or electronic black boxes" and being "mechanical and sure".

He then asks "have the Honda engineers been reading RISKS?" and "Has car design turned a corner because of us?".

These are most interesting questions, especially since Honda has the 4WS in Japan since 1976.

Danny Cohen

> [OK. So an <illogical> conclusion would be that the Japanese invented RISKS prior to 1976. A more sensible conclusion might be that it pays to stick with a good design? But I think there is a tendency to have to keep up with the Joneses in modernizing auto designs and other systems by using computers just to one-up the competition. I'm delighted to hear that Honda might have resisted that in the 4WS. PGN]

Reach out, touch someone

Scott E. Preece <preece%mycroft@gswd-vms.Gould.COM>
Sun, 6 Sep 87 19:56:30 CDT

From: sclafani+@andrew.cmu.edu (Michael Sclafani)
> He says the satellite link won't work until he perfects techniques for
> making the human body act as an antenna. Be he predicts its use by
> parents, pet owners, overseas workers in potential hostage situations,
> Alzheimers's patients and police tracking criminals or parolees.
>
> Does Dr. Man see any hint of Big Brother in all of this?
>
> "Yes, but I don't want to go into it. I'm more into the technical
> aspects."
>
> [What will it take before inventors of technology consider
> implications of their work as part of their responsibilities? MS]

I admit I wasn't there and didn't hear the interview happen, but this sounds to me like a cheap shot out-of-context quote. I don't think there's much question about the desirability of the uses he suggests; it's not unreasonable to promote them despite the potential misuses the moderator and the interviewer fear. There are precious few things in the world that don't have both good and bad uses. It's important to be aware of the potential abuses of the things we create, but it's also important to not be so afraid of them that we sit around creating nothing. Once it is possible to do a thing, and it seems likely that what Dr. Man suggests is not far from feasibility, it will be done. It would be nice for the creator to be one of the first to point out the dangers and to suggest the need for their regulation, but it is unfair to expect someone whose reputation and financial future are tied up in the development of a product to spend as much time plugging its dangers as its virtues. That's what the rest of us are supposed to be doing. One could reasonably say that Dr. Man had done his duty by making his product visible far enough in advance that we can work on controlling it before it is reality.

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

Search RISKS using swish-e

THE RISKS DIGEST

Forum on Risks to the Public in Computers and Related Systems

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

Volume 5: Issue 35

Thursday, 10 September 1987

Contents

Drugs, DES, and the criminal world (A New Connection?)

"Jerry Leichter" <leichter@venus.ycc.yale.edu>
8 Sep 87 15:38:00 EDT

From "Logged On", by Vin McLellan - Digital Review, August 24, 1987, page 87

Anthony Prince Fairchild is doubtless a colorful rogue. Five years ago, when People magazine reported on a dispute between the Aspen sheriff and the Drug Enforcement Administration (DEA) about lax law enforcement in the Colorado resort town, Fairchild stepped forth - not to deny the DEA's allegations that he was running an Aspen "drug factory," but, rather, to defend eccentricity. "It's not against the law to be bizarre," he told People, which featured a photograph of him leaning back against a nude female mannequin he called Christina.

Some may have found Fairchild's face familiar. An engineer by education and

trade, Fairchild had also been a model: His Salem-smoking visage has adorned millions of magazines and billboards. He's now 50 years old, but police still call him a "pretty boy." Last month at a pre-trial hearing in San Jose, Calif., Fairchild curled up on a courthouse bench reading Firestarter, while the curious strolled by to check him out. After all, Fairchild had just had his bail changed from $2.5 million to "no bail" out of fear that he would post the money and disappear. "He looks just like Timothy Leary," said an onlooker, referring to the LSD guru the '60s.

If Fairchild isn't a legend like Leary, it may be because federal authorities have never publicized the extent of their interest in him, even though they've sought him several times over the years. But after being arrested last November with eight kilos of cocaine, $12,000 in counterfeit money and 85 pounds of high explosives, Fairchild became a topic of rumor in Silicon Valley, in the California drug culture and, oddly enough, among the nation's top security consultants as well.

"The guy's got a brain," remarked one California investigator. "You maybe couldn't guess it to see the mess he's in, but he's done a lot of things - legit things - and some say he's just slightly short of being absolutely brilliant." Fairchild's resume indicates success in a half-dozen careers, most recently as an EDP consultant in Silicon Valley. It claims he holds 11 U.S. patents, and states that he was one of the authors of Digital Research's Concurrent PC-DOS. The police say this work record is accurate.

Predictably, Silicon Valley police have been among the first to confront the probleme of criminal enterprises that digitally encrypt incriminating records. "There's one case like that every six weeks around here," noted a local police reporter. "It's become quite common." The method of choice is, of course, the Digital Encryption Standard (DES), the cipher approved by the U.S. government for commercial data security.

Fairchild used a Winterhalter DES board in a DOS micro to keep what police believe to be an extensive diary of the affairs of a "large international drug ring." Local, state and federal narcotics agents are all very eager to gain access to Fairchild's records. Indeed, Santa Clara, Calif., police reportedly used covert FBI funds to have a privately owned supercomputer grind away at cracking the DES-encrypted data.

The attempt was not a big secret. Several EDP security consultants were asked to suggest crypto attacks. What made the DES attack feasible, if still unlikely to succeed, was that the Winterhalter device uses a program to transform a 6-to-16-character password into the 64-bit DES key.

The cops got lucky: With a pass through a full English dictionary, and by culling significant names and such from Fairchild's personal history, they were apparently able to guess three of four passwords that were used to encrypt files stored on his micro.

The passwords were all eight or fewer characters in length, and all in lowercase letters. The diary file continued to elude their efforts, but the police reasoned that if the DES password for the diary was less than eight characters, a "brute force" approach to finding it was possible. A cryptoanalyst who is a leading consultant for California banks was hired to

make the attempt.

The supercomputer may have actually been chewing away when the Justice Department stepped in late last month to confiscate copies of the encrypted diary, presumably as evidence in a federal drug case against Fairchild. This pre-empted local authorities from possibly making the big score.

More on the Irish Tax Swindle (RISKS-4.33)

Jerry Harper <mcvax!euroies!jharper@seismo.CSS.GOV>
Tue, 8 Sep 87 17:01:04 BST

The situation is in fact much worse (and farcical) than seems credible. Firstly, there is no accurate estimate of the size of the fraud, with the revenue preferring to err in low figures. To date the "figure" of 300,000IR (about $4.2m) is being suggested as the *most* accurate. However, no one seriously believes this, least of all tax consultants in the large accountancy firms. Secondly, John's comments about officials causing the disappearance of defaulters files is not quite accurate. Many of the cheques which were altered came from quite respectable companies and self-employed business people -- I am trading on the knowledge of friends who are in taxation consultancy -- it was the deposit time lag in revenue which provided the gateway to the fraud. Between the receipt of a cheque and its lodgement there could be a delay of three months. Finally, and I think this is what John was referring to, the revenue have a "pending file" where information on possible defaulters is kept. By flicking through this file it would have been easy to select the right targets.

P.S. Since the banks no longer have a policy of automatically returning cheques many companies and individuals may be totally unaware that theirs' have been altered.

This is the second major fraud to affect the revenue services here. I reported a previous fraud involving tax repayments to RISKS a few months back. It remains to be seen what comprehensive overhaul of the system will be pursued.

Re Pogo Wins a Free Lunch -- Costs and Liability in Good Systems

Brown <geac!daveb@seismo.CSS.GOV>
8 Sep 87 17:18:32 GMT

The argument probably does not apply to long-lived systems such as operating systems and major suites of applications. Honeywell-Bull found some years ago that the cost of fixing things that could have been done correctly before release was significant, and started a rather successful quality programme, thereby saving themselves money. Most of the areas they saved money were in the maintenance and correction of old, long-running systems, both hardware and software.

Moral: We have met the enemy and ... oh-oh, do we really want this war?

Disclaimer: the above is the opinion of neither Honeywell-Bull nor Geac.

David Collier-Brown, Geac Computers International Inc., 350 Steelcase Road,
Markham, Ontario, CANADA, L3R 1B3 (416) 475-0525 x3279
{mnetor|yetti|utgpu}!geac!daveb

Re: The influence of RISKS on car design?

Benjamin Thompson <munnari!mulga.OZ!bjpt@uunet.UU.NET>
Tue, 8 Sep 87 17:05:59 EST

There seems to be quite a lot of public criticism of steer-by-wire etc. at the moment. Perhaps Honda is just trying to cash in on the current wave of Luddism. Perhaps their electronics don't work. Perhaps they can't produce electronic cars fast enough.

These reasons are all fairly legitimate, and all could explain why Honda plugs the lack of electronics and points out that the car is "mechanical and sure". Honda doesn't have to be particularly safety-conscious to make a profit.

Ben Thompson

Re: Computer Syndrome; Dutch Crime Computer (RISKS 5.34)

Brian Douglass <brian%asci.uucp@RELAY.CS.NET>
9 Sep 87 10:38:47 PDT (Wed)

In regards to the 18 year old that developed "computer syndrome" in Denmark. My question is did the kid develop it because he was working on the computer, as if they pose some inherent social risk, or was the kid already at risk to developing some type of neurosis and because he had a computer it settled on that? Was the kid just as likely to develop a drug habit in an effort to conform and have friends, or possibly take his own life out of frustration and loneliness due to an illogical world he could not fit into. If so, then did the computer save his life by temporarily giving him the logic and structure he craved? Sort of like using a small bomb to destroy a larger bomb, but its still a bomb.

About the inventor who has a developed a telephone receiver that can be implanted behind a human's ear:

Sometimes, no matter how much the potential for good, the dangers can far out weigh them, and therefore the potential good must be denied. A perfect example is the recent Supreme Court ruling for Preventative Detention, that persons can be held with out bail if they are shown to be a danger to the community. The intent was to hold drug pushers and Mafia figures that could easily make bails of 5 or 10 million dollars, and then continue to run their empires, or skip out and not thing twice about it. Well now a D.A. in Florida is using that ruling to hold juveniles that are accused of murder or drugs, or simply have a history of arrests, showing that history as a pattern to prove they are a danger to the community.

Suddenly we have incarceration without trial. Preventative Detention was viewed as having both good and bad effects, but was thought that properly controlled and regulated, it could be used for the good of society without the bad effects. Thomas Jefferson argued for strict interpretation of the Constitution, so that such finely cut interpretations as Preventative Detention could not be legislated by the courts. In our modern society, we feel "smart" enough to be able to maximise the good and minimize the bad.

I agree with the original poster and PGN [You mean "MS"? PGN], sometimes no matter how helpful some technological innovations may be, you must take into account their implications, which are sometimes to grave and it is better left uninvented. I think the article about the Dutch Crime Computer is a perfect example that we are human and do err (even something as *stupid* as dropping your backup system). Could you imagine the chaos if the Dutch allowed Preventative Detention and you couldn't get bail while you waited around for the authorities to straighten things out. That's exactly why Preventative Dentention is supposed to be forbidden by the constitution, but we just think we're so smart. What a glorious 200th birthday present for our constitution.

Brian Douglass, Applied Systems Consultants, Inc. (ASCI), P.O. Box 13301,
Las Vegas, NV 89103 Office: (702) 733-6761
UUCP: {mirror,sdcrdcf}!otto!jimi!asci!brian

Reach out, touch someone [RISKS-5.32]

Brad Miller <miller@DOUGHNUT.CS.ROCHESTER.EDU>
Tue, 8 Sep 87 22:41 EDT

> [What will it take before inventors of technology consider implications of their work as part of their responsibilities? MS]

Umm, jobs that pay regardless of productivity? Brad Miller

University of Rochester, Department of Computer Science 716-275-1118
Computer Science Department, University of Rochester, Rochester NY 14627
miller@cs.rochester.edu {...[allegra|seismo]!rochester!miller}

Reach out, touch someone [RISKS-5.32]

"Richard Kovalcik, Jr." <Kovalcik@MIT-Multics.ARPA>
Tue, 8 Sep 87 12:29 EDT

I don't think the moderator or anyone else is being paranoid here. It is issues like this that make me very glad there are groups like the ACLU. There is a real risk of Big Brother in this. The issues here are very similiar to those of mandatory AIDS testing - when is violating individual rights outweighed by the good to society? Given that such a device would violate existing laws, be easily abusable, and / or be unnecessary because there are other ways of accomplishing the same thing, it should be banned.

Engineers and professionals do have a duty to act responsibly. The moderator is correct.

> [Actually the comment prompting this was marked with "MS", the contributor, NOT the moderator. PGN]

1) The parole laws were not written with the idea that the Government know where the parolee was at every instant in time. To implant a device that did so is certainly violating the existing law and the most probably the parolee's constitutional rights.

2) Parent's should not be allowed to implant this sort of thing. While parents have a responsibility to take care of their children. They should do so by taking an active interest rather than using technology to snoop on their children. Perhaps you think it is OK for parents to bug phones their children might use too? And what about employers recording calls employees make without telling them? Besides, unless there is someway to remove this "wonderful" device onc the person reaches 18, it is subject to being misused later by Government.

3) As to pet owners, anyone who lets their pet roam freely tearing up lawns, breaking into garbage, and playing "chicken" with cars shouldn't be allowed to be a pet owner. I'm sure a lot of people will disagree with me on this one but as far as I am concerned this is another misuse of techology.

4) As for criminals in jail, implanting them would be OK as long as the device was removable after they were released so as not to violate their rights. But, then if it is removable, they could get a shady doctor to do it if they escaped (which is presumably (hopefully?) what you are trying to guard against here).

5) If someone wants to have one implanted to guard against kidnapping that if fine, but I would urge such a person to consider the disadvantages.

Re: Reach out, touch someone

abbott.pa@Xerox.COM <Curtis Abbott>
Tue, 8 Sep 87 18:03:44 PDT

This should be an interesting case for the patent attorneys, because the idea Dr. Man has patented was used as the climactic plot twist in "The President's Analyst", a wonderful film that came out around 1969.

Search RISKS using swish-e

THE RISKS DIGEST

Forum on Risks to the Public in Computers and Related Systems

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

Volume 5: Issue 36

Sunday, 13 September 1987

Contents

Australian Bank Bungles Foreign Exchange Deal

Ken Ross <munnari!mulga.oz.au!kar@uunet.UU.NET>
Sat, 12 Sep 87 11:20:11 +1000

(Quoted without permission from the Melbourne Age, 11 Sept 87, p3)

KEEP THE CASH, JUDGE TELLS MAN WHO WON $335,000 IN BANK BUNGLE

A Fairfield man who made a windfall $335,000 profit after the National Australia Bank made a mistake in quoting an exchange rate on Sri Lankan rupees, won a Supreme Court action yesterday over the money.

Mr Justice Beach dismissed a claim by the bank that Mr Peter George Rogan had taken an unfair advantage of the bank because he must have known the bank had given him the wrong figure.

On 23 December last year, Mr Rogan, who had developed an interest in foreign currency transactions, collected a National Australia Bank list of exchange rates which showed 78.5 Sri Lankan rupees to the Australian dollar.

The figure was confirmed in a telephone call to the bank. He bought rupees to the value of $104,500 and sold them to the Commonwealth Bank the next day for $440,258. (...)

Mr Justice Beach said he had found Mr Rogan to be an honest witness who believed than the Commonwealth and not the National had given him the wrong rate.

The manager of the National Australia Bank's international operations section, Mr Bob Farmer, ... told [Mr Rogan] that the bank had mistakenly entered the exchange rate for Central Pacific francs instead of Sri Lankan rupees into its computer on the day Mr Rogan bought the rupees. Mr Farmer asked if the bank could do a deal to rectify the loss, but Mr Rogan sought legal advice and declined to make any payment to the bank.

Mr Justice Beach said he accepted Rogan's belief at the time that the rupee must have been devalued because of internal strife, and that he believed he had been given the correct figure by the National Bank and that the Commonwealth's much different, unconfirmed figure, on the same day was because it had been slow to catch up and adjust its rate. He described Mr Rogan as an amateur in the world of foreign exchange dealings, rather than an experienced professional. He found that although an irregularity in the exchange rate entered into the bank's computer on 23 December was noticed within minutes, and the rate was withdrawn from use by bank staff, the incorrect figure remained on the bank's computer screens, and Mr Rogan had been given the rate on a number of occasions that day, including the three times that he had bought rupees during the morning, at lunchtime and in the afternoon. Mr Justice Beach dismissed the allegation that Mr Rogan had deliberately split his purchases into a number of parcels each below $10,000 to delay scrutiny of the transaction, and found that it was the National Bank which had first advised him to split deals in an earlier transaction. ...

Computer misses the bus

Peter G. Neumann <Neumann@csl.sri.com>
Sun 13 Sep 87 15:29:13-PDT

30,753 Minneapolis school children were victimized by a misaligned computer merge operation, with almost everyone receiving assignments for the wrong school bus for the new school year. For example, some first-graders were assigned to high school and teenagers were assigned to grade school. In each case the correct bus route for a given name was assigned to the name following in the list. (Thus, just a few children actually received the right assignment -- if two adjacent entries were to be on the same bus for the same school, as in the case of the first one of a pair of twins.)
[Source: Minneapolis Star and Tribune, article by Kate Perry, 25 August 1987, contributed to RISKS by Doug Barry, CDC, Bloomington MN 55420]

Quite a dish subverts Playboy channel

Peter G. Neumann <Neumann@csl.sri.com>
Sun 13 Sep 87 15:15:18-PDT

The Playboy Channel was hit on the evening of 6 September with an attack reminiscent of the Captain Midnight case, when someone ``stepped on their transponder'', i.e., uplinked through the satellite dish antenna. The cable TV program interjection warned viewers to ``repent your sins.''
[Source: San Francisco Chronicle, 10 Sept 87, p. 21]

"Software Glitch Shuts Down Phones in Minneapolis"

<alan@umn-rei-uc.arpa>
Sat, 12 Sep 87 13:10:36 CDT

Thirteen telephone exchanges in downtown Minneapolis went dead about 4 a.m. when a computer program for the Northwestern Bell switching system malfunctioned. About 50,000 customers were affected.

Although some service was restored by 8:35 a.m., Bell spokesman John Walker said the company was electronically limiting use of the troubled exchanges because of a surge in customer demand. That meant that calls were interrupted in some cases by a recorded message explaining all circuits were busy, in other cases by a continuous busy signal.

Walker said the situation was not unlike a freeway traffic jam. "At this point, the wreckage has been cleared, but traffic is still moving slowly because lane use is limited," he said.

The exchanges involved were 332-6, 330,2,3,4,8, 370,2,5. The 348 exchange covers Minneapolis police and fire, but Paul Linnee, directory of emergency communications, said there were no emergency calls that went unanswered.

Walker said the glitch developed while the company was making what he described as a routine equipment modification in one of two computers. Employees were changing computer software that was to extend limits of customer service and add new features, he said.

"We don't know what went wrong with the new software," Walker said. He acknowledged there have been other service interruptions this year, "but nothing of this magnitude."

Walker said Northwestern Bell will continue to limit use of various exchanges "until we are satisfied the system is again stable."

Computer Syndrome

MJackson.Wbst@Xerox.COM <Mark Jackson>
11 Sep 87 09:21:08 EDT (Friday)

The first occurrence of this that I have heard of involved the tab equipment used on the Manhattan Project during the Second World War. The following

account is from "Surely You're Joking, Mr. Feynman!" (Richard P. Feynman, W. W. Norton & Co., 1985); does anyone know of an earlier incident?

> Anyway, we decided that the big problem -- which was to figure out exactly what happened during the bomb's implosion, so you can figure out exactly how much energy was released and so on -- required much more calculating than we were capable of. A clever fellow by the name of Stanley Frankel realized that it could possibly be done on IBM machines. The IBM company had machines for business purposes, adding machines called tabulators for listing sums, and a multiplier that you put cards in and it would take two numbers from a card and multiply them. There were also collators and sorters and so on.
>
> So Frankel figured out a nice program. If we got enough of these machines in a room, we could take the cards and put them through a cycle. Everybody who does numerical calculations now knows exactly what I'm talking about, but this was kind of a new thing then -- mass production with machines. We had done things like this on adding machines. Usually you go one step across, doing everything yourself. But this was different -- where you go first to the adder, then to the multiplier, then to the adder, and so on. So Frankel designed this system and ordered the machines from the IBM company, because we realized it was a good way of solving our problems...
>
> Well, Mr. Frankel, who started this program, began to suffer from the computer disease that anybody who works with computers now knows about. It's a very serious disease and it interferes completely with the work. The trouble with computers is you *play* with them. They are so wonderful. You have these switches -- if it's an even number you do this, if it's an odd number you do that -- and pretty soon you can do more and more elaborate things if you are clever enough, on one machine.
>
> After a while the whole system broke down. Frankel wasn't paying any attention; he wasn't supervising anybody. The system was going very, very slowly -- while he was sitting in a room figuring out how to make one tabulator automatically print arc-tangent X, and then it would start and it would print columns and then "bitsi, bitsi, bitsi", and calculate the arc-tangent automatically by integrating as it went along and make a whole table in one operation.
>
> Absolutely useless. We *had* tables of arc-tangents. But if you've ever worked with computers, you understand the disease -- the *delight* in being able to see how much you can do. But he got the disease for the first time, the poor fellow who invented the thing.
>
> I was asked to stop working on the stuff I was doing in my group and go down and take over the IBM group, and I tried to avoid the disease. ...

"Computer Syndrome"

Simson L. Garfinkel <simsong@cunixc.columbia.edu>
Fri, 11 Sep 87 12:21:32 EDT

This happened to me once, two summers ago, when I was in the middle of a development effort that was taking up about 75 hours of time a week. One day, I was talking to a friend of mine and wanted to change the subject, to what we were doing tomorrow. Almost subconciously, I said the words "cd calendar" (cd being the unix comand to change directory) and saw the letters glowing in light green at the bottom of my visual field.

It started happening a lot. It scared me. Finally, I gave up computers.

-simson

Search RISKS using swish-e

Report problems with the web pages to the maintainer

Search RISKS using swish-e

THE RISKS DIGEST

Forum on Risks to the Public in Computers and Related Systems

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

Volume 5: Issue 37

Friday, 18 September 1987

Contents

Another prison inmate spoofs computer, this one gains freedom

Bill Weisman <
Mon, 14 Sep 87 14:58:44 PDT

From the Los Angeles Herald Examiner, date unknown

FAKE COMPUTER MESSAGE FREED DRUG KINGPIN
By Bill Johnson, Herald staff writer

One or more Sheriff's deputies or civilian employees inside the Los Angeles County Jail aided an alleged cocaine dealer's escape from custody, Sheriff Sherman Block said yesterday.

Block said a computer message directing jailers to release William Londono could only have been generated by one of the nearly 70 deputies and civilians assigned to the jail the morning of Londono's Aug. 25 escape.

It is also clear, Block said, that someone inside the jail assisted Londono once he left his jail cell to avoid a series of checkpoints where his release would have been reviewed and found to be in error.

"The most troubling aspects of this [are that] we don't know exactly how

this happened, and the apparent complicity of someone in this building," Block said.

A team of twelve investigators hasn't yet determined who sent the computer message or how Londono, 23, was able to slip out of the jail virtually unnoticed. Ordered held in lieu of $3 million bail on charges of conspiracy and possession of narcotics for sale, Londono wasn't discovered missing until Monday, six days after his escape.

Any jail employee who could have been even remotely involved is being interviewed, Block said. No action has been taken.

Exactly how Londono was able to bypass as many as five security checkpoints unnoticed remains a mystery, Block said.

"We are able to trace Londono's exodus to a particular point, but haven't been able to go any farther," Block told reporters as he led them from Londono's former jail cell to a holding area where inmates are released. Clothes Londono wore into the jail, for example, are missing, but there isn't any record of him or anyone else retrieving them, Block said.

Investigators on Wednesday determined that the jail's computer system could not have been accessed from outside the building, Block said. It is "highly unlikely" that the release message was sent in error, the sheriff added.

There have been two escapes from the maximum security Central Jail during the past two years. In both instances, inmates switched identification wristbands with soon-to-be-released prisoners, and walked out.

Block said the department has conducted an "almost X-ray type evaluation" of the inmate release process, and have added additional security measures to ward against a similar escape.

"No one is going to leave here today, tomorrow, or at any time in the near future by the same method," the sheriff said.

---

detroit flaps flap

Barry Nelson <bnelson@ccb.bbn.com>
Fri, 18 Sep 87 8:40:10 EDT

According to a Boston Globe article, relatives of persons killed in the recent Detroit crash have filed a suit against the airline. Part of their filing apparently contains claims that the Cockpit Voice Recorder reveals not only the omission of the flap setting during pre-flight checklists (in violation of FAA and nature's rules) but also a discernible voice shouting at the last second, "Oh, [expletive deleted] flaps!" (as in, "oops")

The interesting part is that they go on to discuss the 'circumvention' of a circuit breaker which had de-activated the automatic flaps warnings. Does this mean they could have had multiple systems fed throught the same breaker but

that the flaps warning is the only one that was inadvertently shut off?

In my experience with Aviation Electronics (Avionics), most modern indicators have a big 'OFF' flag, usually orange or red-and-white-striped, dropped across the face when required power is missing (or a blank CRT). Being unfamiliar with complete jet panels, I can only speculate that there is an observable flaps-setting indicator which might be a good place to show subsystem outages. (I recall at one Aerospace company where I worked, they went to great lengths to run test signals through EVERY required harness, connector and subsystem so as to detect outages at various points and interlock man/mission-critical processes, not to mention announcing alarms.)

Is there a System Safety Engineer in the house? Who is responsible for getting the data from one system to the other so as to be easily interpreted as a hazard? Are we to expect an obviously fallible checklist to overcome this?

"This document contains statements of opinion by the author which are not attributable to BBN Communications Corporation or its management."

Barry C. Nelson /Network Consultant/Product Liability and Certifications Group
BBN Communications Corporation / 150 Cambridge Park Drive, Cambridge, MA 02140

AT&T Computers

Peter G. Neumann <Neumann@csl.sri.com>
Fri 18 Sep 87 11:06:48-PDT

Today's Washington Post and yesterday's Chicago Tribune had articles on Herbert Zinn, who apparently broke into a variety of AT&T UNIX systems and copied some sensitive files -- including a pre-release version of an artificial-intelligence program valued at $1,000,000 in potential sales. The articles contain considerable misinformation but again indicate the intrinsic difficulties in making systems secure.

Hackers enter nasa computers

Mike Linnig <LINNIG%eg.ti.com@RELAY.CS.NET>
Tue, 15 Sep 87 20:40 CDT

Ft. Worth Star Telegram:

Reports say West German hackers broke into NASA computer system

FRANKFURT, West Germany (AP) -- Computer hackers broke into NASA's worldwide data network throughout the summer and gathered secret information on space shuttle projects and rocket failures, West German media said Tuesday.

News reports said young West Germans gained regular access to at least 20 computers of the U.S. space agency and had the ability to paralyze the entire network.

The ARD television network said a flaw in the network's security system

allowed the hackers to enter the network from May to September.

Hackers are computer enthusiasts who often try to break into private computer systems for the challenge or for criminal gain.

The NASA system connects more than 1,600 computers worldwide that share information on space research, nuclear physics and molecular biology, ARD said in a report broadcast Tuesday night. The network includes U.S. atomic research facilities in Los Alamos, N.M.

In Washington, the National Aeronautics and Space Administration said in a statement that the tapped network provides unclassified information to university and industry researchers.

"We know of no classified information which can be accessed through the network," the statement said.

The statement said NASA uses a number of computer networks with varying degrees of security to provide "appropriate inviduals" with access to data.

The Hamburg-based magazine Stern reported information similar to the ARD report in an advance telexed to news media Tuesday.

"When I saw "Welcome to the NASA headquarters . . . installation' on my screen, I was a little shocked, to say the least," the magazine quoted one youth as saying.

The Hamburg-based "Chaos Computer Club" said in a statement to news media Tuesday that the youths turned to the club for help when they realized the enormity of their discovery.

The statement said the hackers penetrated the network to show the "unbelievable weaknesses" of the security system and had no interest in the secret data.

The reports did not say how many hackers were involved or where they lived.

Stern said the youths obtained NASA memos to employees on daily space shuttle program updates and on how to deal with the media.

The magazine, quoting one youth's records of computer transactions, said the hackers were able to read users' electronic mail and had the ability to paralyze the entire network.

In one of the most serious security breaches, the hackers obtained NASA information on space shuttle projects, computer security studies and rocket boosters, the television network said.

Scientists in at least eight other countries besides the United States are linked to the computer network. Stern said the system is called the "Space Physics Analysis Network," or SPAN.

Michael Butz, a spokesman for the West German Interior Ministry, said his office had no information about the incidents. The Interior Ministry supervises many police functions in West Germany.

In addition to the NASA computers, the hackers gained access to computers at some of Europe's most sophisticated research institutions, including the European Space Agency in Darmstadt, West Germany; the European Nuclear Research Center in Geneva, an the European Laboratory for Molecular Biology in Heidelberg, West Germany.

Lennart Philipson, director of the molecular biology laboratory, said the institute is re-evaluating its use of the computer network.

"We are considering whether we should restrict our exchange of data with other institutes, even if that might hinder our research," Philipson told ARD.

The hackers said they gained access to the NASA computers by asking for files stored under such key words as "shuttle," "challenger," and "secret," ARD said.

Under those categories, the hackers said they saw data reports on "Shuttle C Study Contracts," a "System Security Study" on computer security, and a study on "Booster Rocket Incidents," the television network said.

The hackers described a step-by-step process of gaining more and more access to the network's computers until they achieved "unlimited access" to all data banks and the ability to "manipulate at will" all information stored there, according to ARD.

ARD said the hackers provided more than 200 pages of documents pertaining to entry into the NASA computers for Tuesday night's television broadcast.

The computer club said the penetration was discovered in August and all organizations who use the network were notified.

So far, no charges have been filed in the case.

Justice Ministry spokesman Henning Gehl said the hackers' actions are punishable by up to three years in prison and fines.

Search RISKS using swish-e

Search RISKS using swish-e

THE RISKS DIGEST

Forum on Risks to the Public in Computers and Related Systems

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

Volume 5: Issue 38

Thursday, 24 September 1987

Contents

Computer crash causes ATC delay

Dave Horsfall <munnari!astra.necisa.oz!dave@uunet.UU.NET>
24 Sep 87 14:55:54 +1000 (Thu)

>From "The Australian", Tuesday Sep 22nd:

"Heathrow crash causes delays (headline)

A software problem last week triggered a computer crash at one of the world's busiest airports, London's Heathrow, causing delays and diversions during a peak period.

The main computer at London's Air Traffic Control Centre broke down for more than three hours at 4.51am on Thursday at a peak period for long-haul arrivals, a Civil Aviation Authority spokesman said.

He insisted there was no danger but said four flights had been diverted to other European cities. Engineers spent more than three hours repairing the computer [system]. The computer at West Drayton, just north of Heathrow, controls all civilian air traffic movement in England and Wales.

The aviation authority spokesman said while the computer was out of commission, air traffic controllers had switched to a manual system and aircraft were ordered to keep a greater separation as a safety precaution."

Comment: why no backup computer?

Dave Horsfall (VK2KFU) ACSnet/CSNET: dave@astra.necisa.oz
NEC Information Systems Aust. ARPA: dave%astra.necisa.oz@uunet.uu.net
3rd Floor, 99 Nicholson St JANET: astra.necisa.oz!dave@ukc
St. Leonards 2064 AUSTRALIA UUCP: {enea,hplabs,mcvax,uunet,ukc}!\
TEL: +61 2 438-3544 FAX: 439-7036 munnari!astra.necisa.oz!dave

---

Risks TO Computers: Man Shoots Computer!

Martin Minow THUNDR::MINOW ML3-5/U26 223-9922 <minow%thundr.DEC@decwrl.dec.com>
23 Sep 87 14:46

From the Echoes-Sentines [?], Somerset County, NJ, Sept. 17, 1987:

GILLETTE RESIDENT IS ARRESTED AFTER SHOOTING HIS COMPUTER

PASSAIC TWP. -- A Gillette man was arrested at his home last Thursday night after he fired eight bullets at his home computer, according to police.

The man, Michael A. Case, 35, of 64 Summit Ave., was arrested shortly after 11 p.m., at his house, when police said they received a report that shots were fired. They arrived at the home to find a .44 Magnum automatic handgun and a shot-up IBM personal computer with a Princeton Graphics System monitor.

The monitor screen was blown out by the blasts and its inner workings were visible, Lt. Donald Van Tassel said on Monday. The computer, which had bullet holes in its hardware, was hit four times while four more bullet holes were found in various areas next to the computer, Van Tassel said.

"The only thing he (Case) said was that he was mad at his computer so he shot it," Van Tassel said.

The handgun, which the lieutenant identified as an Israeli Arms Desert Eagle .44, has "a lot of firepower," he said. "It's a big gun." Case used hollow-point, or dum-dum, bullets, he added.

Case was surprised when police arrested him because he didn't think

he was breaking the law, Van Tassel said. "He couldn't understand why he couldn't shoot his own computer in his own home," Van Tassel said.

Case was charged with recklessly creating a risk and using a firearm against the property of another, because the house is reportedly owned by a relative. The walls were also damaged by the shots, according to police.

He was also charged with unlawful posession of a firearm without a permit, and with possession of illegal bullets, police said.

In addition, Case was issued to summonses, for discharging a weapon in a restricted area and for discharging a single-projectile weapon, police said.

Case spent early Friday morning in the Morris County Jail and was released later in the day on $2,500 bail, according to police.

A Municipal Court appearance is scheduled for today, Sept. 17.

[Strange. I just heard a speaker talking about RIFLING THROUGH FILES, rather than RIFFLING THROUGH FILES. Prophetic? PGN]

An Aporkriffle Tail? (The Squeal of Porchin'?)

Martin Minow THUNDR::MINOW ML3-5/U26 223-9922 <minow%thundr.DEC@decwrl.dec.com>
23 Sep 87 22:01

Date: Mon, 14 Sep 87 23:41:57 CDT
Reply-To: ZEKE@ipfrcvm
Sender: BITNIC LINKFAIL List <LINKFAIL@bitnic.bitnet>
From: ZEKE@ipfrcvm
Subject: IPFRCVM downtime
To: LOCAL DISTRIBUTION <LINKFAIL-LOCAL@omnigate.clarkson.edu>

IPFRCVM - Iowa Pig Farm Research Center will be down tomorrow from 20:00-23:00 for system maintenance. Since we are an end node, nobody will be affected except for us.

It turns out that one of our sows got in through a hole in the wall and had her litter of piglets under our raised floor. The operator on duty got quite a scare when he heard a number of squeals. He assumed we had some massive head crashes and powered down the CPU. Since the squeals continued, we traced it to a corner under our raised floors. We will be off the air tonight so that we can power down again and get the sow and her piglets out from under the floor.

Zeke - System Grunt, IPFRC [Ever litter bit counts!]

The naming of names

Dave Horsfall <munnari!astra.necisa.oz!dave@uunet.UU.NET>
22 Sep 87 08:58:18 +1000 (Tue)

I just heard a report on the radio this morning, while struggling from the foggy depths of sleep. It was one of those filler items they use to take up the space between adverts...

The National Health Service computer in Great Britain sent out letters to several hundred men, inviting them to make an appointment with their gynaecologist for a cervical examination. Apparently, the computer used their first names as the selection basis, and got confused by "foreign" sounding names, and "androgynous" names (their words) like "Lesley". The real kicker is that someone actually responded...

Dave Horsfall (VK2KFU) ACSnet/CSNET: dave@astra.necisa.oz
NEC Information Systems Aust. ARPA: dave%astra.necisa.oz@uunet.uu.net
3rd Floor, 99 Nicholson St JANET: astra.necisa.oz!dave@ukc
St. Leonards 2064 AUSTRALIA UUCP: {enea,hplabs,mcvax,uunet,ukc}!\
TEL: +61 2 438-3544 FAX: 439-7036 munnari!astra.necisa.oz!dave

[I imagine there were a lot of acervic responses from insulted males, as well as requests for appointments that never got kept. Ann Onymous]

<Robert Aitken>
Mon, 21 Sep 87 11:35:42 EDT

<mcgill-vision.UUCP!uhura.ee.mcgill.ca!rob@larry.mcrcim.mcgill.ca>
To: risks@csl.sri.com
Subject: Aliases, SINs and Taxes

The Montreal Gazette reported an interesting problem over the weekend (9/19/87). It seems that a Ms. Josee Gagnon, a 19 year old student from Repentigny (near Montreal), had sent in her tax return and expected to get a modest refund from a summer income of roughly $4000. Revenue Canada informed her, however, that she owed them an additional $400 in taxes. The tax department claimed that this was the tax owed on two additional jobs in Matane, over 300 miles away. Apparently there is another Josee Gagnon, with the same birthdate, living in Matane, and the government issued the two of them the same social insurance number (SIN). A Revenue Canada spokesman says the mixup is due to an "unlikely coincidence".

The newspaper does not identify the cause of the problem, but it appears that the Canadian government uses name and birthdate to key social insurance numbers. Perhaps they should think about including birthplace as well.

Rob Aitken, larry.ee.mcgill.ca!spock!rob

Risks in the Misuse of Databases

Prof Cliff Jones <@NSS.Cs.Ucl.AC.UK,@cs.ucl.ac.uk:cliff@unix.cs.man.ac.uk>
Mon, 21 Sep 87 8:14:18 BST

It might be that my paranoia comes from the title of the article:

> "TV cheats uncovered"

The article (in the London Times) runs:

> "The Post Office has uncovered the address of every home in Britain without a television licence as it begins its biggest crackdown against licence dodgers, it was disclosed yesterday.
>
> An estimated 1.4 million people avoid paying the licence fee each year.
>
> Until now attempts to catch licence dodgers have been hampered by lack of precise information, but the Post Office has used a computer system to pinpoint evaders.
>
> A spokesman said: `For the first time the computer now has a record of every address in Britain without a television licence. There is no doubt we are closing in on evaders. It may well be a record year for prosecutions' "

A (simple ?) diff operation between 2 databases and you have it: my name on a list of potential lawbreakers! (My strange behaviour (not owning a TV) could be used as evidence for all sorts of other oddities!) I am worried because I think these databases were not really designed for this purpose.

Cliff Jones, Manchester

Sprint Sues Hackers

Dan Epstein <hpperf1!de@hplabs.HP.COM>
Mon, 21 Sep 87 10:26:14 pdt

I was reading notes, and I came across the following information.
I, however, can not vouch for the accuracy or authenticity.
Dan Epstein, Hewlett-Packard, {hplabs, ucbvax}!hpda!de

Relay-Version: version Notes 2.7.5 (840 Contrib) 87/2/5; site hpcupt1.HP.COM
From: gcm@mtgzz.UUCP (g.c.mccoury)
Date: Wed, 16 Sep 87 20:27:41 GMT
Date-Received: Thu, 17 Sep 87 08:58:32 GMT
Subject: Sprint sues hackers
Message-ID: <3067@mtgzz.UUCP>
Organization: AT&T, Middletown NJ
Path: hpcupt1!hpda!hplabs!sri-unix!husc6!hao!oddjob!gargoyle!ihnp4!homxb!mtuxo!mtgzz!gcm
Newsgroups: att.general,misc.headlines

From Communications Week 8/31/87:

US SPRINT SUES OVER ALLEGED THEFTS

US Sprint Communications Co., Kansas City Mo., late last week filed federal lawsuits in three states, seeking more than $20 million in damages in connection with an alleged multistate long distance theft ring. The suits were filed in U.S. district courts in Kansas City, Seattle and Los Angeles. The thefts allegedly involved hackers who used computers to identify US Sprint authorization codes, and individuals and companies that sold the codes and used them to place unauthorized telephone calls. Defendants named in the lawsuits are Frederick Deneffe III and Burton Andrews of the Portland, Ore., area; Paul Lindahl, Ralph Purdy III and Kenneth Sheridan, all of the San Francisco area; and Gyan Syal and Karlheinz Mueller of the Los Angeles area. Charges previously were filed against some of the defendants by federal authorities. The defendants allegedly did business under various company names, including Unitel Systems Inc., California Discall Inc., and Hello America. US Secret Service agents, with the help of US Sprint investigators, seized hundreds of illegally obtained US Sprint authorization codes, along with computer equipment, in a series of raids in Kansas, California, Washington and Texas. Bernard Bianchino, the US Sprint attorney heading company actions against such offenders, said the stolen codes were used to place more than $20 million worth of long distance calls.

Grover McCoury, ATT IS/Communications Laboratories

Re: Reach out, touch someone (RISKS 5.32)

Bob English <lcc.bob@CS.UCLA.EDU>
Tue, 15 Sep 87 11:49:36 PDT

> [What will it take before inventors of technology consider
> implications of their work as part of their responsibilities? MS]

Individual action cannot stop these developments; it can at best slow them. Few technological applications are so remarkable that only one person could conceive of them. Even if Dr. Man avoided this line of research, someone else would take it up eventually, someone who either didn't care about, didn't notice, or sought the Big Brother applications of this new technology.

This century has seen many successful totalitarian societies, and none of them needed Dr. Man's devices to function. His devices, while they may facilitate or strengthen such regimes, will not create them of themselves. The problem of totalitarianism is a human problem and requires a human solution.

This is not to say that scientists have no responsibility in these matters. "Advances" such as Dr. Man's carry with them grave risks, and it is the

responsibility of all people who care about such issues to make sure those risks are known, and to do what they can to prevent the risks from becoming realities. Part of that responsibility is to stem the flow of such threats by avoiding the research that develops them. By doing so, we give society extra time to learn about and to deal with these threats.

But that will not win the fight. It is only a part of it. --bob--

Search RISKS using swish-e

Report problems with the web pages to the maintainer

Search RISKS using swish-e

THE RISKS DIGEST

Forum on Risks to the Public in Computers and Related Systems

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

Volume 5: Issue 39

Saturday, 26 September 1987

Contents

Another Australian ATM Card Snatch

Dave Horsfall <munnari!astra.necisa.oz!dave@uunet.UU.NET>
16 Sep 87 13:55:24 +1000 (Wed)

>From the Sydney edition of "The Australian", Tue Sep 15:

``Human error blamed in great ATM card snatch

A fault in the Commonwealth Bank automatic teller machine on Saturday - which impounded more than 900 Mastercards - has been attributed to human error. But technicians are continuing to investigate the system's software.

Mastercard users were confronted with "No account, card retained" messages on Saturday morning when they attempted to use their cards in Commonwealth Bank or Westpac ATM's, and 921 cards were impounded.

The Commonwealth Bank's acting general manager for retail banking, Mr John Koch, said that although the Mastercard reference file had been loaded into the system on Friday, "it did not take". "Every night the Mastercard file is updated and loaded ... but as the computer did not take the Mastercard file on Friday night it had no record of the accounts. The next step was for the ATM's to impound the cards, which is a very desirable security feature. The principle of the system is fine, it's just the practical application that went wrong." ''

Went wrong indeed! It left hundreds of customers without cash for the weekend. The article went on to say that it was "almost certain the fault lay with incorrect loading commands by a human operator".

Readers will recall a previous snafu with Westpac ATM's, when they went live with a new version of software. The repercussions are still rippling...

Dave Horsfall (VK2KFU) ACSnet/CSNET: dave@astra.necisa.OZ
NEC Information Systems Aust. ARPA: dave%astra.necisa.oz@uunet.UU.NET
3rd Floor, 99 Nicholson St JANET: astra.necisa.OZ!dave@ukc
St. Leonards 2064 AUSTRALIA UUCP: {enea,hplabs,mcvax,uunet,ukc}!\
TEL: +61 2 438-3544 FAX: 439-7036 munnari!astra.necisa.OZ!dave

---

AT&T Computers Penetrated [More]

jcmorris@mitre.arpa <Joe Morris>
Fri, 18 Sep 87 12:24:43 EDT

Washington Post, 18 September 1987, p. F1, ff., (C) [filtered by Joe]

YOUTH ACCESSES AT&T'S COMPUTERS

A 17-year-old Chicago high school student using a personal computer in his bedroom broke into AT&T's computer systems around the country, stole $1 million worth of sophisticated software and was "on the verge" of being able to disrupt the company's telephone network, according to federal prosecutors.

The youth also appears to have gained access to AT&T computers at two military bases: the NATO Maintenance and Supply Headquarters in Burlington, N.C., and Robins Air Force Base in Georgia, an Air Force logistics command center, according to prosecutors. The computers did not store classified or sensitive material, they said.

[Comments on other attempted penetrations, including the Washington Post's own computer system.]

[...AT&T says:] "We view this as a kind of Yuppie vandalism [...].

[The investigation involved] agents from the Secret Service, the FBI, and the Defence Criminal Investigative Service [...].

[The youth's lawyer] said yesterday that the youth "categorically denies doing anything that he should not have been doing. I can assure you that

my client had absolutely no sinister motives in terms of stealing property. Right now we're very much in the dark as to what this is all about."

[...] several persons familiar with the case said the incident was highly embarrassed [sic] AT&T and showed potentially serious lapses in its security. [...] AT&T officials believe the incident does not demonstrate flaws in the company's security system but in the failure of its employees to follow proper security procedures. [...] "We're saying the locks are pretty damn good, but we need to remind people to close the door."

On-line Robotic Repair of Software

"Maj. Doug Hardie" <Hardie@DOCKMASTER.ARPA>
Tue, 15 Sep 87 12:27 EDT

The following is taken from Business Week, Sep 7, 87 page 113.

THIS SOFTWARE ROBOT FIXES SYSTEMS - WHILE THEY'RE RUNNING

With computer systems growing more pervasive and complex, maintenance is a mounting headache - especially as networks rope together more unrelated brands of equipment. Finding and fixing problems too often turns into a finger-pointing contest among vendors.

But suppose there were a robot technician residing in software that could worm its way freely through the system, periodically "exercising" the diagnostic programs provided for each piece of equipment. Imagine that this software robot is "smart" enough, when it discovers problems, to run the applicable repair routines. Command Technologies Inc., a Boston startup, claims its SoftRobot software does this and more. For example, if a hard disk crashes, the SoftRobot might move data to another system, restart the first drive, and restore the data. The program, says Command President Franco Vitaliano, "fools the system into thinking that a person is doing the work." As a last resort, the system summons a human. SoftRobots, which cost about $2,500 for workstation-level systems, are being evaluated by a dozen computer companies.

Re: An Aporkriffle Tail (RISKS-5.38)

Michael Wagner +49 228 303 245 <WAGNER%DBNGMD21.BITNET@wiscvm.wisc.edu>
Fri, 25 Sep 87 11:29 CET

> IPFRCVM - Iowa Pig Farm Research Center ...

What was not mentioned in RISKS is that this message strongly [and pungently] suggests that the site IPFRCVM is fictitious: it appears in none of the current tables for BITNET to which I have access.

[Note: APOCRYPHAL = of doubtful authenticity. Add this one to Chernenko@MOSKVAX. (I have edited Michael's note slightly.) PGN]

Risks in the Misuse of Databases? [RISKS-5.38]

Brint Cooper <abc@BRL.ARPA>
Fri, 25 Sep 87 0:45:15 EDT

> A (simple ?) diff operation between 2 databases and you have it: ...
> Cliff Jones, Manchester

Correct me if I'm wrong but isn't this info used merely for the enforcement authorities to decide where to search for unlicensed TV receivers? They won't arrest you solely because you're not in the database, will they?

What's the alternative? When we uncover risks or abuses in the use of computer systems, we are obliged to compare these with the risks or abuses in accomplishing the same job without computer systems. The only effect of the automated databases is to help find unlicenced TV sets more quickly than by searching manually. In either case, some number of such sets will be found. Only the numbers differ.

[Cliff's notes that he is indeed paranoid and abviously STRANGE for not owning a TV, plus the statement that they have uncovered EVERY HOME WITHOUT A LICENCE -- irrespective of the presence of a TV -- are indeed illustrative of the more general problem of drawing inferences from information gathered out of context from networks of networks of databases. This is by no means a new problem, and has been discussed here in the past. It gets more difficult to control HUMAN misuse as the scope of the search widens. But the key point is that the linking together of databases for purposes other than their original intent does raise social questions.
(Cliff and friends -- help! The network is suddenly no longer accepting your CS.UCL.AC.UK relay.) PGN]

SDI Simulation

Steve Schlesinger <steves%ncr-sd.SanDiego.NCR.COM@sdcsvax.ucsd.edu>
21 Sep 87 16:34:20 GMT

The following recently appeared on modsim distribution, a mailing list on issues in simulation. I thought RISKS would appreciate the point that the simulator understood the complexity of the simulation task, but not the fact that the simulation is easy compared to the real problem of SDI control.

I've deleted the name of the poster, but not his organization.
Steve Schlesinger, NCR Corporation <Usual Disclaimer - I speak only for myself>

To: modsim-dist@sunset.prc.unisys.com
From XXXX@mitre-bedford.ARPA Fri Sep 18 10:56:49 1987

This has been touched onb before but I'd like to see if some more discussion can be generated. I am involved in developing a distributed simulation of a large SDI communication network.

The two approaches to distributed simulation are the roll-back, TimeWarp and the Chandra Misra message passing. I am leaning very heavily towards the Chandra Misra model mainly because of my misgivings about the TimeWarp model. These misgivings are

1) The amount of memory devoted to maintaining a history one can roll back to. The networks we will be modelling will consist of 500 to 1500 satellites, each with at least 10 queues and/or buffers. Checkpointing could be expensive.

2) The roll-back support would have to be developed from scratch. We would be building a complicated software support environment along with the simulation itself.

3) Debugging in such an environment would be a BEAR. We would be catching bugs in the roll back support, bugs in the simulation itself and bugs in the interaction between the support and the simulation, I can see us tracing a message, not being sure its valid or not and then seeing it being "taken back" and not being sure whether the "take back" is valid - oooh gives me chills.

I'd welcome some discussion on these points (or others)

[All articles for inclusion in modsim should be sent to ..!isdcrdcf!sdcjove!modsim OR "modsim@cam.unisys.com"]

Ethical dilemmas and all that..

<LIN@XX.LCS.MIT.EDU>
Fri, 18 Sep 1987 15:37 EDT

All of us have been exposed to the question of whether or not an engineer should consider the implications of his or her work. The question is usually posed in the following way: Should an engineer work on certain projects if the social implications of that project are negative? Questions like "Can (or will) the project be used to do bad things?" become relevant. This is one kind of ethical dilemma.

Another type of ethical dilemma arises when a similar question is asked of policy makers. Do policy makers have an ethical responsibility to prevent engineers from having to confront ethical dilemmas?

At first, I thought the answer was clear -- Don't ask someone else to do something you wouldn`t do yourself. But that's insufficient. I am willing to pay someone to provide food for me (I'm not vegetarian), and that involves things I am unwilling to do myself.

The problem for a policy maker comes from the fact that he must plan for an uncertain future. That means hedging against the possibility that his judgments might be wrong. As a defense policy maker, for example, it may be that he cannot imagine any circumstances under which a certain weapon might be used. Should he then not think about how to use that weapon at all? Or

should he spend a little bit of time, money, and energy thinking about possible ways it could be used in the event that his judgment is wrong? If the latter, that could mean that he would have to ask someone to think about doing things that he (the policy maker) would never want done and moreover could not imagine wanting done.

It is clear to me that the policy maker should not spend a lot of money etc and thus ask many people to confront ethical dilemmas. But should he ask a few? I invite comments.

[This could lead to an interesting, albeit rather free-form, discussion. Responses to Herb (cc: RISKS), please. PGN]

Search RISKS using swish-e

Report problems with the web pages to the maintainer

Search RISKS using swish-e

THE RISKS DIGEST

Forum on Risks to the Public in Computers and Related Systems

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

Volume 5: Issue 40

Monday, 28 September 1987

Contents

Yet another "hackers break MILNET" story, some interesting twists

Jon Jacky <jon@june.cs.washington.edu>
Mon, 28 Sep 87 10:53:17 PDT

The following story appeared in the paper almost two months ago. Since it hasn't been reported in RISKS before, I thought I would pass it along. It is interesting mainly because of comments by DDN spokesmen and consultants. While taking pains to assure reporters that classified data is not kept on the network, they also made the point that information on MILNET might be useful "in aggregrate" - foreign intelligence agencies could piece together information from diverse sources to infer some classified information. This same argument has been used to justify restrictions on presentations of

non-classified material judged "sensitive." I find it interesting that this doctrine is invoked in this case; it mitigates against the usual attempt of the breakin victims to assure the press that the breakin was really no big deal. I think usually it is the press that exaggerates the importance of these incidents, but clearly the blame must be shared here. Incidentally, it appears that the breakins were accomplished by taking advantage of well-known holes in typical Unix security practices that have been explained at length in RISKS, in articles in CACM and lots of other places, probably including THE WEEKLY READER by now.

Here are some excerpts from the August 3, 1987, story in THE SEATTLE TIMES, p. A5. It is attributed to NEWSDAY:

'HACKERS MAY HAVE CRACKED PENTAGON COMPUTER SYSTEM'

NEW YORK - Young computer users under investigation in connections with recent seizures of equipment and records in Brooklyn and elsewhere have penetrated ... a network of computers used by military researchers and bases - MILNET - that the Pentagon said in 1983 it overhauled to prevent casual breakins and data vandalism.

A Pentagon computer specialist, Lt. Col. Taylor Landrum of the architecture and planning group of the Defense Department's Defense Data Network ... said the methods the youths described were plausible ...

He and other security experts emphasized that the Pentagon does not keep classified data on the network. But he agreed taht some data on the network was sensitive and could be useful "in aggregate" - by piecing together the work product of many people - to foreign intelligence agencies." ...

A 15-year-old West Coast youth who calls himself "Solid State" (said) "They (the Secret Service) told me I was a national security problem. They said I could have comitted treason and stuff." The Secret Service will not comment on the case.

(End of excerpts. There was a lot more largely accurate information on the difficulties of network security. - Jon Jacky)

Military role for software sabotage cited in big CHICAGO TRIBUNE story

Jon Jacky <jon@june.cs.washington.edu>
Mon, 28 Sep 87 11:16:21 PDT

The following story got a full page, with artwork, inside the front section of the Sunday, Sept. 20 1987 SEATTLE TIMES:

A NEW BATTLEFIELD: SOFTWARE WARFARE - RISING FORM OF COMPUTER SABOTAGE MAY BE NEXT GREAT MILITARY EQUALIZER

by Scott A. Boorman and Paul R. Levitt - Chicago Tribune

If members of the John Walker spy ring could betray their positions of trust

to the Soviets for nearly 20 years, what could US adversaries do to sabotage-quietly, from the inside - the complex computer programs on which US weapons vitally depend? ...

Software warfare - attacking the software that controls or operates such weapons - may be the cheapest, simplest, and most effective way to cripple US defenses. Such sabotage is coming of age as a new type of systematic warfare, which can be waged far removed from space and time from any battlefield to influence not only combat outcomes but also peacetime balances of power ...

Given a host of recent US spy scandals, it is easy to envision a computer programmer offering, if the price is right, to add or modify critical lines of software to benefit a hostile country...

Given its scale and mission ... it is SDI that merits special scrutiny in light of software concerns. ... The effort to develop and coordinate all the necessary SDI software seems destined to involve several thousand software professionals working alone, working over many years. ... The extreme complexity of SDI software also suggests that significant bugs may be nearly impossible to trace - even after some future software saboteur is caught...

Software warfare's relative cheapness .. may make it the next great military equalizer. ... (It) certainly lies well within the grasp of any number of agressive lesser military poweers with the means to buy insiders to plant crippling bugs ...

It is vital to bring software warfare into focus in broad arenas of US national security planning.

(End of excerpts)

The story cited an article by the late Rear Adm. Henry Eccles in the June 1986 Naval War College Review. It did not cite other sources who have mentioned this idea, including David Parnas and the French authors of a thriller titled SOFTWAR that appeared in translation in the USA a few years ago.

The article also claims "American teenagers using home computers have developed the capability to alter orbits of commercial satellites, as demonstrated by a recent incident in New Jersey." Surely this must be an exaggeration?

- Jon Jacky

$80,000 bank computing error reported in 'Ann Landers'

Jon Jacky <jon@june.cs.washington.edu>
Mon, 28 Sep 87 10:24:34 PDT

The following appeared in the "Dear Ann Landers" advice column in the Seattle Post Intelligencer, Saturday Sept. 26 1987, under the headline, "HERE'S PROOF THAT COMPUTERS CAN GOOF UP." It is interesting for several reasons: the correspondent's apparent prior unfamiliarity with computer bug stories,

and the antics of the service people. I pass it along without permission from the newspaper or from Ann Landers:

Dear Ann Landers:

I've read one too many articles that proclaim "computers don't make mistakes."

Five of us would like to challange that statement. We made an audit of one month's business and found that accounts were out of balance by more than $80,000. Everything was on the computer. We worked far into the night and finally discovered that 21 bank deposits were on the printout but the total was dropping one.

A programmer was called in. He worked seven days and called another from the home office. They worked another two weeks.

They had the original entries re-entered 50 times. More than 150 reprintouts were made, but the same error kept occurring. They admitted it was not a human error.

The machine was crated and sent back to the factory. A replacement arrived within days. We were asked not to discuss this matter with anyone.

- It Happened in Texas

(End of excerpt from 'Ann Landers' - Jon Jacky)

Add Vice to the Loveworn

Scot Wilcoxon <umn-cs!sewilco@datapg.MN.ORG>
26 Sep 87 15:50:15 CDT (Sat)

Three men in Rochester, Minnesota, have been arrested after they telephoned the police for a prostitute. After a family complained that men were calling their new phone number and asking for women, Northwestern Bell agreed to give the number to the Rochester Law Enforcement Center. If a call comes in and a vice team is available, a female officer wired for sound is sent out.

Lt. Barry Fritz, supervisor of the vice unit in Richfield, MN, says they have not used abandoned outcall service numbers because of the difficulty of finding such numbers and possible data privacy violations.

The above information is from a well-balanced article by Bill McAuliffe in the 9/25 Minneapolis Star Tribune, pg 14B.

Scot E. Wilcoxon, Data Progress sewilco@DataPg.MN.ORG +1 612-825-2607

Concorde tires burst: RISKS without the automatic system

Henry Spencer <mnetor!utzoo!henry@uunet.UU.NET>
Mon, 28 Sep 87 18:17:33 EDT

Flight International for Aug. 29 reports that a British Airways Concorde burst five tires on landing at JFK on Aug. 11. Nobody was hurt and no emergency evacuation was necessary, but two engines were later replaced as a precaution because they had ingested debris. (If the Concorde was being designed over again, in hindsight one definitely would not put the landing gear directly in front of the engine intakes!) The interesting part is the reason for the tirebursts: the main hydraulic system was down due to a "minor fault", leaving the brakes on the standby hydraulic system... which has no antiskid control. The disturbing aspect here is that the crew evidently had come to rely completely on the antiskid braking system. Unless, perhaps, the pilots were unaware that they were back to "dumb" brakes -- seems unlikely -- it's disturbing that they made such a drastic error in braking procedure. These were not second-rate pilots, by the way; my understanding is that the Concorde is the most sought-after assignment in BA, and it is likely to have BA's best crews.

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

Risks of hot computers [sic!]

Mark Brader <msb@sq.com>
Sun, 27 Sep 87 05:40:49 EDT

I wouldn't ever pay for a copy of the Toronto Sun, but if I find one abandoned on the subway, I flip through it. In this morning's Sun, I found this rendering of a UPI article:

U.S. Computers Snatched

Stockholm (UPI) -- Swedish police issued a national alert for two stolen U.S. microcomputers classified as strategic materials, fearing a thief would sell them to Soviet-bloc countries. The two Micro-Wax 2 computers were stolen Saturday from Uppsala University.

Mark Brader utzoo!sq!msb
[If only Icarus had had one of them! PGN]

Re: Risks in the Misuse of Databases? [RISKS-5.38]

Ross Patterson <A024012%RUTVM1.BITNET@wiscvm.wisc.edu>
Mon, 28 Sep 1987 13:41:11 EDT

>From: Brint Cooper <abc@BRL.ARPA>
>Correct me if I'm wrong but isn't this info used merely for the enforcement
>authorities to decide where to search for unlicensed TV receivers? They
>won't arrest you solely because you're not in the database, will they?

I can't speak about the UK, but here in New Jersey, any evidence obtained through such a database cross-match would probably be ruled inadmissable in court. The N.J. Supreme Court has held on several occasions that a search warrant (as would be needed to actually enter a house to find a TV set) cannot be issued on the basis of such "fishing expeditions". Rather, the Court expects the person requesting the warrant to show "probable cause" that a crime has been committed, thus justifying the search. The legal requirements to demonstrate probable cause do not allow generalizations, such as "No persons without a TV License may own a TV set, therefore all persons not owning TV Licenses should be searched." The preferred form is to limit the request to those suspected of committing a crime, as in "No persons without a TV License may own a TV set, therefore all persons whose homes openly sport a TV antenna and who do not own a TV License should be searched." This, of course, means that the database cross-match provides the police with no additional homes to be searched, since they still must identify the homes in question by some criminal criteria.

>What's the alternative? When we uncover risks or abuses in the use of
>computer systems, we are obliged to compare these with the risks or abuses
>in accomplishing the same job without computer systems. The only effect of
>the automated databases is to help find unlicenced TV sets more quickly than
>by searching manually. In either case, some number of such sets will be
>found. Only the numbers differ.

More important is the ability to derive a new datum from the conjoining of existing data. Specifically, the cross-matching of a list of all addresses in Berlin with a list of all Christians in Berlin would yield a list which would contain all Jews in Berlin. This is a far more efficient method of locating groups of people that Hitler had at his disposal, and as you say, provides quicker results than by searching manually. Only the numbers differ.

Before the flamers start complaining about the use of loaded terms, my point is that ethics and social responsibility, while largely ignored in computing to date, are rapidly becoming critical to our continued survival as a planet and a race.

Ross Patterson, Rutgers University

[SDI] Simulation (RISKS-5.39)

Freedman <jfjr@mitre-bedford.ARPA>
Mon, 28 Sep 87 13:57:38 EDT

I was/am quite offended by the use of my letter out of context to advertise the uncertainty of star wars. I said nothing about SDI itself nor about my beliefs. All I was talking about were detailed problems in a distributed simulation. That letter was part of a larger discussion. Taking what I said out of context, and making assumptions about my perceptions, judgements and opinions on the real thing and then indicating surprise and indignance over the result is intellectually dishonest and unfair. I think the issues raised by SDI are important enough not to need this sort of

puerile potboiling.

Jerry Freedman,Jr

Re: An Aporkriffle Tail [On the detection of bogus mail site names]

William R. Somsky <wrs%pupthy2@princeton.edu>
29 Sep 87 01:38:54 GMT

Of course the site "IPFRCVM" must be ficticious!
There might be an "Iowa HOG Farm Research Center"
but never an "Iowa PIG Farm Research Center"! :-)

"Billy Bob" Somsky - A transplanted Iowan

William R. Somsky Physics Dept ; Princeton Univ
wrs@pupthy.Princeton.EDU PO Box 708 ; Princeton NJ 08544

Search RISKS using swish-e

THE RISKS DIGEST

Forum on Risks to the Public in Computers and Related Systems

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

Volume 5: Issue 41

Wenesday, 30 Sept 1987

Contents

CHANGE IN RISKS SITE Effective Immediately

<Neumann>
30 Sep 87 08:00:00

```
  ========================================================================
  | This is the VERY LAST RISKS FROM F4.CSL.SRI.COM.  Our Foonly F4 will  |
  | no longer be maintained after 1 October 1987.  Incoming mail can be   |
  | addressed as before, or to RISKS@SRI.COM and RISKS-Request@SRI.COM,   |
  | as appropriate.  The FTP site has changed to SRI.COM.  For the        |
  | immediate future RISKS operations will be moved to SRI.COM.  Thanks to|
  | David Poole for keeping our Foonly in excellent shape all these years.|
  ========================================================================
```

Life-critical use of a spelling corrector

Dave Horsfall <munnari!astra.necisa.oz.au!dave@uunet.UU.NET>
30 Sep 87 16:52:59 +1000 (Wed)

The following appeared on the back page of one of Australia's more outrageous computer publications, "Computing Australia", 21st Sept 1987:

> ... Blame it on the computer.
>
> An unfriendly computer has been held responsible for a "potentially lethal error" involving a Mafia loan collector.
>
> A New York paper inadvertently put the `heavy' in the running for a pair of custom-fitted concrete shoes when it identified him as a "ruthless informer".
>
> According to a published retraction (and apology!), a writer on the paper had actually typed "ruthless enforcer" - but the computer system's spelling checker liked it the other way.

And I thought the worst you could expect from a "computer error" was a bill for a million dollars!

Now, this particular publication (Computing Australia) is not known as the "computer gutter press" for nothing, so I would appreciate any comments from indigenous Americans...

Dave Horsfall (VK2KFU) ACS: dave@astra.necisa.OZ
NEC Information Systems Aust. ARPA: dave%astra.necisa.OZ@uunet.UU.NET
3rd Floor, 99 Nicholson St UUCP: {enea,hplabs,mcvax,uunet,ukc}!\
St. Leonards NSW 2064 AUSTRALIA munnari!astra.necisa.OZ!dave

AT&T Computers Penetrated

<Richard.S.D'Ippolito@sei.cmu.edu>
Monday, 28 September 1987 15:21:02 EDT

AT&T's attitude that the break in was just 'Yuppie vandalism' and the defense attorney's comments on motives make me wonder when, if ever, the view of computer crimes will merge with society's view of other property crimes: we have laws against breaking and entering. You, as property owner, don't have to provide 'perfect' security, nor does anything have to be taken to secure a conviction of unauthorized entry. That conviction should be easy. Also, using CPU resources (a demonstrably saleable product) amounts to theft. There still seems to be the presumption that computer property, unlike other property, is fair game.

I do not imply that we should relax our security efforts -- merely that we deserve the same legal presumption that our imperfectly protected systems and work are private property subject to trespass and conversion protection.

Satellites and Hackers

<pgarnet@nswc-wo.ARPA>
Tue, 29 Sep 87 13:54:36 edt

>The article also claims "American teenagers using home computers
>have developed the capability to alter orbits of commercial
>satellites, as demonstrated by a recent incident in New Jersey."
>Surely this must be an exaggeration?

Yes, it is a case of misinformation. The 17 July 1985 issue of the New Jersey newspaper "The Star-Ledger" reported

>The unidentified juveniles, arrested following an intensive
>computer theft probe by South Plainfield, county and federal
>authorities, also participated in elaborate schemes to steal
>merchandise using stolen credit card numbers and reprogrammed
>an American Telephone and Telegraph (AT&T) communications
>satellite to disrupt phone conversations on two continents,
>according to Prosecutor Alan A. Rockoff.

An article in the same paper two days later, on 19 July 1985 reported

>The seven, who are strangers to each other but communicated
>regularly on part of a nationwide computer "billboard" network
>for hobbyists, are accused of stealing computer informational
>services, stealing telephone services, disrupting satellite
>communications and exchanging information on how to make
>explosives and tap into Pentagon and defense contractors over
>coded phone lines.

Time magazine reported on July 29, 1985 (p 65)

>The New Jersey episode assumed heroic proportions when
>Middlesex County Prosecutor Alan Rockoff reported that the
>youths, in addition to carrying on other mischief, had been
>"changing the positions of satellites up in the blue heavens."
>That achievement, if true, could have disrupted telephone and
>telex communications on two continents. Officials from AT&T
>and Comsat hastily denied that anything of the sort had taken
>place. In fact, the computers that control the movement of
>their satellites cannot be reached by public phone lines. By
>week's end the prosecutor's office was quietly backing away
>from its most startling assertion, but to most Americans, the
>satellite caper remained real . . .

This New Jersey case is not very "recent", but seems to be the one being referred to. If anyone knows of another more recent New Jersey "satellite caper", please fill me in.

Paul Garnett

Re: Risks in the Misuse of Databases? [RISKS-5.40]

P. T. Withington <PTW@YUKON.SCRC.Symbolics.COM>
Tue, 29 Sep 87 10:48 EDT

From: Ross Patterson <A024012%RUTVM1.BITNET@wiscvm.wisc.edu>

>From: Brint Cooper <abc@BRL.ARPA>
>Correct me if I'm wrong but isn't this info used merely for the
>enforcement authorities to decide where to search for unlicensed TV
>receivers? They won't arrest you solely because you're not in the
>database, will they?

I can't speak about the UK, but here in New Jersey, any evidence obtained through such a database cross-match would probably be ruled inadmissable in court.

How does this jive with a vaguely remembered NPR article of last week that described how people who had failed to register for the draft were found by matching social security numbers? The gist of the article was similar in spirit to the UK television article: the social security database is searched for draft-age candidates and those registered with the selective service are subtracted out. All this despite existing laws that state SSN's are to be used only for social security and not as a identification number. Unfortunately, few people know the law only states you have the right to refuse to give your SSN and must instead be assigned some other ID number (which presumably would be different for each service and prevent this type of abuse). If you "voluntarily" give your SSN, you essentially waive your privacy rights. The only service I have dealt with that treated my refusal to give my SSN as a normal operation was the Massachusetts Registry (I won't bore the list with a diatribe on its faults which far outweigh this one feature). Most services simply will refuse to deal with you when you decline to give your SSN, whether they understand the law or not.

Re: Risks in the Misuse of Databases

Scott E. Preece <preece@mycroft>
Tue, 29 Sep 87 09:40:28 CDT

Ross Patterson:
> The preferred form is to limit the request to those suspected of
> committing a crime, as in "No persons without a TV License may own a TV
> set, therefore all persons whose homes openly sport a TV antenna and who
> do not own a TV License should be searched." This, of course, means
> that the database cross-match provides the police with no additional
> homes to be searched, since they still must identify the homes in
> question by some criminal criteria.

It's a little more complicated than that, though: My understanding is that it is possible to detect the use of a TV set from outside the house. Is it then permissible for the authorities to use the database cross-match to identify houses to check (since the check does not involve a search)? Or is that the fruit of the poisoned tree?

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

Re: Risks in the Misuse of Databases? [RISKS-5.38]

J M Hicks <cudat@DAISY.WARWICK.AC.UK>
Wed, 30 Sep 87 15:35:00 bst

Disclaimer: this information came to me third-hand. Bear this in mind.
This happened several years ago.

A friend once told me that his parents had been threatened with court action for not having a television licence, when they did not have a television. They protested to the licensing authorities, which backed down apologetically. It looked as though everyone in town who didn't have a licence was being threatened.

This could have been a mere clerical mistake, of course.

J. M. Hicks, Warwick University. (a.k.a. Hilary)

Search RISKS using swish-e

Report problems with the web pages to the maintainer

Search RISKS using swish-e

THE RISKS DIGEST

Forum on Risks to the Public in Computers and Related Systems

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

Volume 5: Issue 42

Monday, 5 October 1987

Contents

Credit Markets: computer interest is high!

Jerome H. Saltzer <Saltzer@ATHENA.MIT.EDU>
Fri, 2 Oct 87 09:47:01 EDT

Buried near the bottom of the daily report of Credit Markets on page 29 of the Friday, October 1, Wall Street Journal is the following intriguing paragraph:

> "The rate on federal funds, or reserves that banks lend each other overnight, averaged 7.6%, down from 8.38%, according to Fulton Prebond (U.S.A.) Inc. At one point Wednesday, the rate was as high as 30% because of a computer problem, the Fed said."

That one somehow sounds a little scarier than usual. Does anyone have any facts?

Jerry

Telephone computers that work

Buckaroo Banzai <wex@MCC.COM>
Fri, 2 Oct 87 09:27:08 CDT

A short blurb in today's paper reports that the Pac Bell computers logged over 300,000 phone calls in the six minutes after the earthquake. The system appears to have degraded gracefully under the excessive load - the only problems reported were delays in getting a dial tone.

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

[As always, it is nice to see success stories. On the other hand, the call volume that resulted was enormous all day -- and various LA exchanges were down completely for quite some time. By late evening it was still almost impossible to get some calls through to LA. PGN]

Computer Services as Property

<portal!cup.portal!Isaac_K_Rabinovitch@Sun.COM>
Sat Oct 3 10:57:35 1987

A recent message in the RISKS Forum raises an issue that I think needs more careful discussion. The opinion expressed was similar to many I've heard in the last few years, in its complaint that people regard the theft and disruption of computer services more tolerantly than theft and vandalism of "other forms of property."

I think such opinions are based on the mistaken belief that society and the law regard the property holder's rights as absolute and final. I'm not a lawyer or a serious student of social mores, but it's obvious to me that both law and society recognize that a property holder has an obligation to take reasonable measures to prevent tresspass, vandalism, and theft.

Society in general has little sympathy for people who are careless with their property, as many system administrators have sometimes been. An administrator who accidentally publishes all his user passwords (something that I've actually seen happen!) is certainly like a person who absent mindedly leaves his front door unlocked.

Providers of computer services are right to be frustrated with the slugish way judges and legislators apply existing moral and legal concepts to the new technology. But they should be aware that existing legal concepts are not entirely on their side. Consider the laws of easment, for example.

They should also not pay excessive attention to the arguments of

defense attorneys, whose jobs obligate them to take a very narrow view of these problems.

None of this excuses the Matt and Ally fans who think that fouling up a Big Corporation's operations is just a fun prank. And it certainly doesn't justify more serious forms of hooliganism and brigandage. But system administrators should not feel that society is giving them a special bum deal.

Computer Services as Property (Re: RISKS-5.41)

<"Arthur_Axelrod.WBST128"@Xerox.COM>
5 Oct 87 08:21:16 PDT (Monday)

In RISKS DIGEST 5.41, Richard.S.D'Ippolito@sei.cmu.edu writes:

> " . . . the defense attorney's comments on motives make me wonder when, if ever, the view of computer crimes will merge with society's view of other property crimes: we have laws against breaking and entering...

I think we all agree with the fundamental premise, i.e. that information is a form of property and is entitled to the same protection as any other form of property. However, there is a difference between information property and tangible property that complicates the issue and may be responsible for much of the confusion in society's view and the ambiguity in current law.

To extend the analogy, in real property ("real" as in "real estate") the law makes a clear distinction between "fully private" property and "places of public accommodation." (I may not have the legal terms right, but you get the idea.) I'm allowed to walk at will through a shopping mall, for example, even if I have no intention of buying anything. I can come in out of the rain, use the rest rooms, sit on a bench and warm up, and not be subject to prosecution for breaking and entering. The "resources" that I use, bench space, warm air, rest rooms, etc. are "saleable items" in the sense that the mall owner has to pay for them, and recovers that cost in rent from merchants.

On the other hand I can't simply walk into your house at will. Not even if you leave the door wide open. Furthermore, your house doesn't have to have a sign saying "private property" on it. If I did that, I would be subject to charges of trespassing, illegal entry, and burglary, or at least attempted burglary. You wouldn't be required to show that you had taken any special measures of protection, let alone had "perfect security." It is assumed that everyone knows that a house is private property and furthermore it is assumed that everyone is capable of recognizing a house.

That's the point. Through long custom and usage, we have all come to be aware of the distinction between private places and places of public accommodation. The key phrase here is "long custom and usage." The problem that we face with computer security is that society has not yet had a chance to form a conceptual model of the distinction of what is or

is not a private information resource. The era of the widely accessible computer is hardly ten years old.

Education is one part of the process. One of the functions of the security measures that we computer operations people take must be in a sense educational. People who literally don't know any better, because they've never been taught, must be told, in one way or another, "Look here, this is private. Keep out." Schools, government, etc., have a responsibility, too, of course, but ultimately, computer professionals have the greatest stake and must accept the fact that we must take the lead. Some day, the view of computer crimes will indeed merge with society's view of other property crimes, but we better face the fact that it may not be soon.

Art Axelrod, Xerox Webster Research Center

JOINing on public access data -- and insider trading (Re: RISKS-5.41)

Brent <itm!brent@csl.sri.com>
1 Oct 87 19:53:39 GMT

The recent talk in this group about cross-correlating public databases for questionable purposes reminds me of the method used to catch insider trading on the NYSE.

Above "the floor" is a computer room that constantly monitors the movements of stocks. If a stock moves up or down more that a certain percentage of its selling price in a given day, or if more shares trade hands than normal, an alarm sounds. The analysts then cross-correlate that stock with all available press releases, wire service reports, and stock offerings to try to determine if there is a valid reason for this movement. If no reason can be determined, the incident gets investigated further. The buying and selling stockholders get cross-correlated with the members of the board and all employees of the company in question. They also cross-correlate all known data about the parties in question: club memberships, professional societies, civic organizations, to try to determine if any contact was likely. If these joins come up positive, the case gets investigated by old-fashioned "legwork." The above information was related in an NPR story as the insider trading scandal was breaking a while back.

I have long suspected that if "big brother" were to come into being, it wouldn't be created by the government. The government is far to big, slow, and open to public inspection. If "big brother" is to be created, it will probably be done by private enterprise, as above. But it's not just the "big-wigs" of the NYSE. It's you and me being cross-correlated as below:

There are companies known as "list brokers." These companies buy and sell names and addresses. Everyone notices that once you get on one "junk mail" list, you soon get mail from a plethora of other

organizations. Your name has been brokered. All types of organizations from credit-card companies to non-profit fund raisers buy and sell lists. The price depends on the quality of the name, from a cent or so for inactive names to upwards of a dollar a name for high quality lists. The average is about 10 to 15 cents. How do the most profitable companies make money? By cross-correlating. One of the largest list brokers has taken the census information and run cluster analysis on a wide range of socio-economic scales. The result is a clustering of the nation into 17 groups. These have colorful names like the "pickups and shotguns" cluster, and the "money and brains" cluster. Now suppose a shotgun shell maker wants to drop a direct-mail piece to new prospects. What kind of list should he buy? The list broker pulls up the "pickups and shotguns" profile and determines that a greater than average number of people in that segment also own electric freezers, so they sell the shell maker a list of names of people who returned warranty cards for freezers. Viola! Everyone makes money: the freezer manufacturer who sold the freezers, then sold the names to the broker, the broker who re-sold the names at a mark-up (the value added being the cross- correlation he ran) and the shell maker who stands to sell more shells than to an unqualified list.

Add another wrinkle: the intelligent set-top cable converter. This is an individually addressed converter used for "pay per view" cable. You see a good movie will be on HBO tonight. You call your cable company. They turn on HBO for you house tonight so you can see RAMBO or whatever. Thus they collect information on you as to who wants to see what movie. Another new feature is the "people-meter." At 8:07 p.m. tonight, the central cable computer sends out a "poll" message. The set-top captures what channel it's currently tuned to and over the next 24 hours, all the little set-tops report back to the home office. This can go into the database as well. It's only a matter of time until this information is merged with the list-brokers profile. Now we have a complete demographic profile of your household: Area of town, cost of house, number of incomes, favorite TV shows, most recent major purchases, etc., etc.

I claim if "big brother" is to be, it will come from the private sector for marketing reasons, motivated by profit. There is legislation in the works to prevent the cable companies from selling information. But will the set-tops encrypt the data they send? If not, a simple passive tap could generate reams of data. The potential for invasion of privacy is large here, simply because of the scale of the mailing list and cable systems. Also by the nature of the beast, the correlations are done on a huge scale, hence only approximate in many cases, so the potential for mismatches is large.

Brent Laminack

TV Detectors

"Lindsay F. Marshall" <lindsay%kelpie.newcastle.ac.uk@NSS.Cs.Ucl.AC.UK>
Thu, 1 Oct 87 16:39:55 BST

Detecting a TV inside a house is easy, and is a process that has been refined over the years to cope with such things as multiple occupancy and high-rise flats etc. I have also heard of people being sent letters about TV licences when they had no TV, but I don't think they were any more threatening than your average government letter. I would doubt very much that the search for licence evasion is as simplistic as has been suggested - the impression I get is that the letters sent by mistake tend to be caused by people with no TV moving into a new house where the previous occupant did have one. I would suspect that the address is a more important part of the check than the occupant, rather like some credit validation schemes, where information concerning previous occupants can blight you for up to 6 years - I got caught by this recently, and to add insult to injury, the information was not even correct! The previous occupant had been summonsed AFTER he had vacated out house, but for some reason was still listed as being at our address...however the companies involved sorted this out very fast and very politely.

Lindsay

TV Detectors

"Ian G. Batten" <BattenIG@CS.BHAM.AC.UK>
Thu, 01 Oct 87 12:16:56 BST

My parents (who do not have a TV) get a letter every year stating that they do not hold a license and then giving a list of reasons as to why this may be so (just bought the TV, forgotten it expired, etc). Nowhere on this note does it suggest the possibility that they don't have a TV! This letter can only be being generated by cross-matching some "list of everyone" with a "TV license-holders list", as they have had the house from new in 1961 and have never had a TV in that time. [I can't remember when radio licenses were subsumed into TV licenses and waived for the non-TV 1% of the population; I'm too young :-)]

ian

---

detecting TV's

David A Honig <honig@BONNIE.UCI.EDU>
Thu, 01 Oct 87 15:50:22 -0700

I don't know how easy it is to detect TV's from a distance (though I suspect anything using heterodyning is detectable from the emissions from the IF oscillator), but I recall a story about detecting satellite-TV thieves:

The satellite TV company drove down a street with a RF signal analyzer and detected the emissions from rooftop dishes. Each house with a dish tuned to the (im)proper frequencies was sent a harsh letter describing the (fairly accurate, in this case) evidence against them. Apparently this was effective (partially it was a publicity-motivated crackdown, the satellite company wanting to show that they could catch "signal-stealers").

Confusing Input Request in Automatic Voting Systems

<SBQBEB%HLERUL57.BITNET@wiscvm.wisc.edu>
Mon, 5 Oct 87 16:11 N

Last election in 1986 several cities in Holland used voting machines in order to keep a count of the votes for the candidates of the various parties.

It appeared that several voters were confused by the lay-out of the buttons and inadvertently choose the wrong candidate by pushing the button at the wrong side of the candidate's name. This was discovered in the little village of Katwijk because suddenly a conspicuous great amount of people voted for a very left-wing party (whereas in other years the vast majority votes for the very right-wing "Gereformeerde Partij").

Eke van Batenburg, Instituut v.Theoretische Biologie, Groenhovenstraat 5
2321BT Leiden (tel.071-132298) Holland

[They could tell left from right among the parties, but not among the buttons. PGN]

DIAC-88 CALL for PAPERS

Douglas Schuler <douglas@BOEING.COM>
Fri, 2 Oct 87 14:49:20 pdt

Call for Papers

DIRECTIONS AND IMPLICATIONS OF ADVANCED COMPUTING
DIAC-88 St. Paul, Minnesota August 21, 1988

The adoption of current computing technology, and of technologies that seem likely to emerge in the near future, will have a significant impact on the military, on financial affairs, on privacy and civil liberty, on the medical and educational professions, and on commerce and business.

The aim of the symposium is to consider these influences in a social, economic, and political context as well as a technical one. The directions and implications of current computing technology, including artificial intelligence and other areas, make attempts to separate science and policy unrealistic. We therefore solicit papers that directly address the wide range of ethical and moral questions that lie at the intersection of science and policy.

Within this broad context, we request papers that address the following suggested topics. The scope of the topics includes, but is not limited to, the sub-topics listed.

RESEARCH DIRECTIONS DEFENSE APPLICATIONS

Ethical Issues in Computing Research AI and the Conduct of War
Sources and Effects of Research Funding Limits to the Automation of War
Responsible Software Development Automated Defense Systems

COMPUTING IN A DEMOCRATIC SOCIETY COMPUTERS IN THE PUBLIC INTEREST

Community Access Computing for the Handicapped
Computerized Voting Resource Modeling
Civil Liberties Arbitration and Conflict Resolution
Risks of the New Technology Software and the Professions
Computing and the Future of Work Software Safety

Submissions will be read by members of the program committee, with the assistance of outside referees. The program committee includes Steve Berlin (MIT), Jonathan Jacky (U. WA), Richard Ladner (U. WA), Bev Littlewood (City U., London) Nancy Leveson (UCI), Peter Neumann (SRI), Luca Simoncini (U.Reggio Calabria, Italy), Lucy Suchman (Xerox PARC), Terry Winograd (Stanford), and Elaine Weyuker (NYU).

Complete papers, not exceeding 6000 words, should include an abstract, and a heading indicating to which topic it relates. Reports on in-progress or suggested directions for future work will be given equal consideration with completed work. Submissions will be judged on clarity, insight, significance, and originality. Papers (4 copies) are due by April 1, 1988. Notices of acceptance or rejection will be mailed by June 1, 1988. Camera ready copy is due by July 1, 1988. Send papers to Professor Nancy Leveson, ICS Department, University of California, Irvine, Irvine, CA 92717.

Proceedings will be distributed at the symposium, and will be available during the 1988 AAAI conference. The DIAC-87 proceedings are being published by Ablex. Publishing the DIAC-88 proceedings is planned. The program committee will select a set of submitted papers to be considered for publication in the Communications of the ACM.

For further information contact Nancy Leveson (714-856-5517) or Doug Schuler (206-865-3226).

Sponsored by Computer Professionals for Social Responsibility, P.O. Box 717, Palo Alto, CA 94301.

Risks of receiving RISKS -- BITNET users BEWARE [ANOTHER REMINDER]

<JFPJ%CORNELLA.BITNET@WISCVM.WISC.EDU>
30 September 87 20:45 EDT

[For those of you on BITNET, you should be aware of the instructions for the automatic self-maintaining mailing list indirection (which apparently is going to change in the near future). PLEASE DO NOT send any mail to the designated RISKS address except the properly formatted SUBSCRIBE and UNSUBSCRIBE messages. All other messages get rebroadcast to the BITNET RISKS community, and then I get complaints... Instructions upon request,

if you have lost them. BUT, I am suddenly getting notices from LISTSERV that I (not YOU?) can add YOU using ADD (not SUBSCRIBE?)... Grumble... Update on the new forwarding when available. PGN]

It seems that computers indeed aren't flawless - especially as regards automated redistribution of the RISKS Digest on BitNet. For several weeks (ever since I subscribed, in fact) I have been getting various messages, none of which has to do with RISKS (mostly subscription requests &c). Wondering if something was amiss, I sent a message to the address used for BITNET subscription. Much to my surprise, when I logged in several days later, I found 12 messages waiting for me. They were typically from people experiencing the same difficulties, but two held the key to the problem.

It seems that the address for BITNET subscription/distibution has a very limited intellect. If it receives mail of the proper for (ADD ... or DELETE ...), it is processed. Any other mail is assumed to be a RISKS issue, and is distributed to the subscribers. Needless to say, my query was treated as a RISKS Issue, and was subsequently distributed.

-jfp

Search RISKS using swish-e

THE RISKS DIGEST

Forum on Risks to the Public in Computers and Related Systems

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

Volume 5: Issue 43

Tuesday, 13 October 1987

Contents

IRS Accidentally Imposes $338.85 Lien On Reagans

<DowJones@andrew>
Tue, 6 Oct 87 10:12:30 -0400 (EDT)

WASHINGTON -- The IRS acknowledged that last summer it accidentally placed a lien against President and Mrs. Reagan.

The error, by a trainee in the Austin, Texas, IRS district, followed a demonstration of the agency's electronic lien system. Despite an IRS policy against using the names of real people in training, an instructor used the Reagans as a hypothetical example.

Later, when the trainee was practicing, she pushed the wrong button, accidentally filing a lien of $338.85 at the Travis County courthouse in Austin. The incident was recently reported in the Kiplinger Tax Letter.

Although the lien was discovered and rescinded, it will remain a permanent entry in the Travis County Court records because the courthouse doesn't routinely remove a record of a lien even after it's been lifted. But the IRS notice releasing the lien also remains part of the record.

Since the entry had assigned the Reagans a fictitious address and Social Security numbers, "there was never any real danger of a real lien being filed," said an IRS spokesman.

Ellen Murphy, IRS public affairs director, said the IRS has taken steps to prevent a repeat occurrence, "including appropriate disciplinary action where needed."

Another ARPANET-collapse-like accidental virus effect

Jeffrey R Kell <JEFF%UTCHP1.BITNET@WISCVM.WISC.EDU>
FRI, OCT 9, 1987, 1:39 PM

[Response from Jeffrey to my message to him regarding the ARPANET collapse, article by Eric Rosen, Software Engineering Notes 6 1, January 1981. PGN]

Extremely interesting, and personally relevant. I wrote the "RELAY" package for Bitnet which is essentially a distributed message service of real-time interactive messages as opposed to mail. A "chat" if you prefer the Compuserv example, only there are multiple Relays across a broad geographic area (Bitnet is store-and-forward). Each Relay services users in its local area, and exchanges messages with its neighbors, who exchange redistribute locally and further send to neighbors, etc. It's a very simple flooding algorithm since it is a closed network with no loops.

At any rate, a missing edit check and an innovative student discovered that Relay allowed him to sign on to channel "1.0"; the code is written in a high-level language and it asserted 1.0 to be a whole number. The message packet was created and with the "1.0" channel prefix header and was then flooded to the neighboring Relays to update their user tables. With that done, it then goes back to a ready state, which is handled by a front-end Assembler routine. The assembly code tried to download the user table, in the process tried to pack and convert to binary the "1.0" value, which abended on an data exception. Meanwhile, the neighbors receive the update, flood it, and try to go ready. Abend for same. The net result: 36 Relays on 4 continents abended almost simultaneously.

Moral of the story: If it's garbage in, eat it :-) /Jeff/

Computers and civil disobedience

Prentiss Riddle <rutgers!im4u!woton!riddle@uunet.uu.net>
6 Oct 87 22:27:47 GMT

We've heard much about computer crime for personal gain, about vandalism

committed by crackers out for kicks, and now "software warfare" in which a superpower might attempt to undermine an opponent's warfighting capability by sabotaging its software. But has there been any discussion of real or hypothetical civil disobedience by computer?

A loose definition of "civil disobedience" might be nonviolent lawbreaking by morally motivated individuals, often in what they perceive as obedience to a "higher law" (e.g. constitutional or international law or a religious or ethical principle). A few famous examples of CD in the non-computer world include Rosa Parks' refusal to move to the back of a bus, occupation of power plants and weapons facilities by anti-nuclear protesters, and "Plowshares" actions in which priests and nuns have destroyed components of nuclear weapons.

It seems to me that as the computerization of society continues, the idea of engaging in civil disobedience via computer is bound to come up more often. Some computer CD might resemble ordinary computer crime and sabotage except for the motivation of the individuals carrying it out. I've heard folklore about politically motivated crackers for years now; do RISKS readers know of any actual examples?

Other forms of civil disobedience might be engaged in by members of the general public with no special expertise in computers, especially as computerized communications systems become more pervasive. For example, rather than physically occupy a street or building, protesters might clog up a computer network by engaging in bogus transactions. (This has already been done with telephone systems: reputedly some fundamentalist right organizations have had to abandon their toll-free numbers after it became a common pastime in certain gay and countercultural circles to call them up and waste their money. This was known as "the Falwell game.")

Like all civil disobedience, computer CD raises many ethical and tactical questions. Can anyone out there think of any particularly frightening or promising scenarios for computer CD looming on the horizon?

--- Prentiss Riddle ("Aprendiz de todo, maestro de nada.")
--- Opinions expressed are not necessarily those of Shriners Burns Institute.
--- riddle@woton.UUCP {ihnp4,harvard}!ut-sally!im4u!woton!riddle

---

YAPB (yet another password bug)

Geof Cooper <imagen!geof@decwrl.dec.com>
Tue, 6 Oct 87 17:56:53 pdt

I just discovered that the much-touted BSD4.3 release of Unix silently truncates passwords to 8 characters. I found this out by having an easier time guessing a password for an account than I thought I would -- because the user name had 8 characters and the password was the user name with a suffix.

Let's get this info out to the user community... BEWARE!

- Geof Cooper

News Media about hackers and other comments

Jack Holleran <Holleran@DOCKMASTER.ARPA>
Wed, 7 Oct 87 23:37 EDT

Two recent articles from "The Capital", the daily newspaper for Annapolis, Maryland. Both are re-typed without permission and condensed. Names of accused are deleted.

= = = = = = =

October 6, 1987
Teen computer 'hacker' to be tried as adult (Page D1)
By Lorraine Ahern -- Staff writer

A Hanover youth who police claimed used a home computer to charge thousands of dollars worth of electronic equipment to stolen credit card numbers will be tried as an adult, a judge ruled yesterday.

[NAME DELETED], 18, is accused of ordering more than $6,400 worth of computer accessories and radar detectors, and having UPS deliver them to his family's home address last summer.

Circuit Court Judge Eugene Lerner granted a prosecutors request that [NAME DELETED], who turned 18 last month, be charged and tried as an adult for felony theft.

"It's not a kid walking into a 7-Eleven and walking out with a Snickers bar in his pocket," Assistant State's Attorney Eugene Whissel argued. "It's a mature crime for an adult --- a sophisticated crime."

... non-related discussion ...

[NAME DELETED] mother said that [...] her son became depressed and "obsessed" with the home computer he had set up in his bedroom.

"Initially, I did think that it was good," said [his mother], who testified that she was unaware of any UPS-credit card scheme. "Getting him down to even eat with us ... he was on it all the time. I knew it was not healthy. I even took the plugs at times."

[He allegedly confessed that he got the equipment using an illegal MasterCard number from a Brooklyn, NY computer contact through an electronic bulletin board. The Secret Service is "already" being investigated by the Secret Service.]

During the same period last spring when state police began investigating [NAME DELETED]' computer activities, police in Baltimore County arrested a number of computer "hackers" in the Annapolis [MD] area and charged them with gaining free illegal access to long-distance telephone service.

end of article

'Hacker' pleads guilty (page A13)
By Lorraine Ahern -- Staff writer

An Annapolis [MD] man pleaded guilty yesterday to stealing long-distance telephone service using his home computer, which a judge ordered destroyed.

In a case that began a year ago with raids on the homes of sever computer "hackers" in Annapolis and the Baltimore suburbs, J. Scott Meenen [...] pleaded guilty to theft of service in Baltimore County Circuit Court.

Meenen, a 28-year-old former audio-visual repairman [...], was put on probation and ordered to pay back $477 to MCI Telecommunications for stolen long-distance service.

Police claimed that Meenen had operated an electronic bulletin board known to a circle of computer hackers as "The British Exchange." Using an automatic sequential dialing device, police said, the hackers would hit upon MCI code numbers and then, sharing them on the bulletin board, use those numbers for free long-distance calls.

MCI began to pick up on the unauthorized use of the codes through a switching station at Towson [MD (about 30 miles north of Annapolis], and police ultimately traced the calls to computer telephone lines at several addresses.

MCI spokeswoman Pamela Small said yesterday[,] thefts that cost the long-distance carriers an estimated $500 million in 1986 alone have decreased.

Under Chesapeake & Potomac's [local phone provider] gradual conversion to "equal access," long-distance carriers such as Sprint or MCI will no longer need to assign code numbers for customers to dial.

Equal access, which Ms. Small said is now 80 percent complete, means that the subscriber can simply dial the long-distance number itself, as they would if they used AT&T.

end of article

Comments: During the 1987 National Computer Security Conference in Baltimore, Detective McCleod (sp?) of Arizona discussed that he likes to visit and arrest youthful hackers when they turn 18. This was based on a bad experience in the court system for a case against a 14 year youth. This youth was successfully prosecuted and convicted to some community service and a 2 page, hand-writted, double-spaced paper. The "convicted" youth then demanded his computer equipment back and got it. He was not obligated to pay back the

fraud. [I remember $14,000 but I could be wrong.]

Maybe police and judicial activities like this will bring back the original definition of "hacker".

If "equal access" reduces losses, maybe it's time to invest in those companies.

Personalized Technology Side-effects

Scot Wilcoxon <umn-cs!sewilco@datapg.MN.ORG>
7 Oct 87 08:15:14 CDT (Wed)

"Computer Watch Aids Body ID 06-Oct-87

BLAUVELT, N.Y. (AP) - Police used a computerized wristwatch that had phone numbers stored in its memory to identify a man whose body was found last week in a park. ... State Police Inspector William Sprague said police tracked down acquaintances of Bly's through his wristwatch, which had their telephone numbers programmed into it." (remainder of article describes the death)

RISKS DIGEST was recently discussing implanted transmitters. A computerized wristwatch is not as threatening to one's privacy as an implanted transmitter. But other personalized technology can pose threats to the users, or benefits to society: A recent drug arrest near Minneapolis led to several more arrests after police investigated a phone number from the memory of the drug dealer's cellular phone.

These examples show the electronic equivalent of scraps of paper in pockets, except that people are presently not usually aware of them nor know how to alter them.

Medical technology with serial numbers can also be used for identification, at least for dead people. An anonymous live suspect with a surgical implant would pose a dilemma, although there already have been court cases of evidence (bullets) in living people. Simple pacemakers with a serial number are already numerous. Near-future technology may cause more complications, such as a computerized nerve replacement implant with a memory of recent motions (ie, pulling a trigger or route recently walked).

Scot E. Wilcoxon, Data Progress sewilco@DataPg.MN.ORG +1 612-825-2607

(Peter: Pacemakers DO have serial numbers. I called Medtronic and theirs do. I assume other manufacturers also have them in case of recall.)

Anonymity and high-tech

Nic McPhee <mcphee@ratliff.cs.utexas.edu>
Thu, 8 Oct 87 18:57:36 CDT

This is in response to the recent discussion of TV licenses and Brent

Laminack's comments concerning "Big Brother".

One of the greatest guarantees of privacy is anonymity. For example, there's hardly a house made that absolutely can't be burgled, and most would be rather trivial, and police and crime experts have often stated that the best protection is anonymity - looking less interesting than someone else. Similarly, were someone *really* interested in you and your habits it probably would not have been difficult for them to learn a great deal about you - where you live, work, shop, relax, etc. But anonymity protected you, because it was just too expensive to do this checking on a random basis with no justification.

That's all changing now, because simple operations on readily available databases can find the needle (us) in the haystack of teeming masses with very little expense. And a degree of anonymity is lost. Many of us are still as indistinguishable as before, but not all. Going back to the example of burglary, the potential exists for some smart crooks to do some neat cross-referencing of addresses of people who buy (or even read about) high-ticket items that are small in size and easily fenceable (cameras, electronics, jewelry, etc. - many readers of this group would probably qualify) and target them. Going one step further, they might eliminate from this list people with burglar alarms or a high chance of owning a large dog, or come better prepared for such contingencies.

One aspect of this that I find particularly disturbing is its affect on the notion of "innocent until proven guilty". Barring widespread, indescriminate government harassment, one of your biggest protections against being hassled by the government was your anonymity. If you're just an average Joe, then there's no reason for the government to suspect you of anything, gratuitously assuming guilt until convinced otherwise. There was no return on the investment from the government's standpoint. Not anymore. Now they can assume you're guilty ("You don't have a TV license, and you must own a TV, therefore you must be guilty of not obtaining a needed license".) in some subtle ways in their uses of database cross-referencing, and get a pretty good return on their (minimal) effort.

Nic McPhee (mcphee@ratliff.cs.utexas.edu)

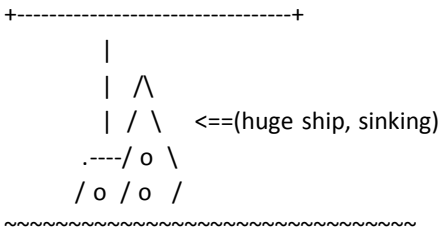
[Incidentally, for those of you wondering how you can detect whether someone's TV set is in use, read Peter Wright's SPYCATCHER. It is easily available outside of the U.K., and I understand copies are creeping into Britain at a great rate. PGN]

Naval Contemplation [Humor] [A slip of a chip can sink a ship? PGN]

Don Chiasson <G.CHIASSON@DREA-XX.ARPA>
Thu, 8 Oct 87 00:46:20 ADT

Seen in Office Management and Automation, Sept.87, p. 4:

```
+---------------------------------+
|I've found the flaw, sir!        |
|It's in this little computer chip.|
```



(Well, their graphics were better than mine.....)

Search RISKS using swish-e

THE RISKS DIGEST

Forum on Risks to the Public in Computers and Related Systems

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

Volume 5: Issue 44

Thursday, 15 October 1987

Contents

Costly computer risks

Gary A. Kremen <89.KREMEN@GSB-HOW.Stanford.EDU>
Tue 13 Oct 87 17:28:10-PDT

From The Wall Street Journal of October 13, 1987 page 47:

"But the DOT [Direct Order Transfer - a computer system that makes large-scale stock trading faster and more efficient] system isn't foolproof, either. Mr. Nelson [whom the article is about] said he heard a story about a man who pushed his DOT button intending to buy one $25 million package of securities. When he didn't get a confirmation of his order, he hit the button again, and then again and again. A few minutes later, he received four confirmations showing that he had just bought $100 million of stock."

The article itself is very interesting for those who are looking for another view on a topic that has been discussed is RISKS for some time - computer assisted stock trading and "program trading."

Re: News Media about hackers and other comments

Amos Shapir <nsc!taux01!taux01.UUCP!amos@Sun.COM>
14 Oct 87 14:22:44 GMT

Jack Holleran <Holleran@DOCKMASTER.ARPA> writes:
> An Annapolis [MD] man pleaded guilty yesterday to stealing long-distance
>telephone service using his home computer, which a judge ordered destroyed.
^^^^^^^^^^^^^^^^^^^^^^^^^^

Talk about computer phobia! This must be the silliest court decision since a boat was put to the gallows in the 17th century!

Amos Shapir, National Semiconductor (Israel)
6 Maskit st. P.O.B. 3007, Herzlia 46104, Israel Tel. +972 52 522261
amos%taux01@nsc.com (used to be amos%nsta@nsc.com) 34 48 E / 32 10 N

Mailing Lists

"Lindsay F. Marshall" <lindsay%kelpie.newcastle.ac.uk@NSS.Cs.Ucl.AC.UK>
Thu, 15 Oct 87 10:28:59 BST

Only 17 categories of people!! That's not very sophisticated - Britain is broken down into 45 distinct groups by one of the companies who sell mailing lists. They have a very neat acronym for this system which eludes me at the moment. They have also introduced a new system called "Monica" which classifies people by their first names (Monica is a slang pun - I don't know if it is meaningful in the US). The idea is actually very obvious - certain first names are popular at certain times and don't get recycled at regular intervals so having a first name like "Florence" tends to indicate that you are older, whereas "Darren" is a younger person's name. I don't know how this would apply in the US, but the short extracts I have seen are strikingly accurate when compared with people I know. It does fall down on names like "John" and "David" which are perennial favourites, and also on very unusual names or he/she names like Lindsay of course.

Also on the subject of mailing lists, there was an interesting letter in the Guardian from someone who received a batch of junk mail about investments,

expensive holidays and subscribing to the Tory party. The man has no money and has been unemployed for 2 years. The letters started arriving six weeks after he had a letter printed in the Times newspaper...

Lindsay

[I wouldn't want to Harm Monica, but a moniker is a nickname, as is Nick, and Phil (Harmonica?). PGN]

Re: Anonymity and high-tech

Brint Cooper <abc@BRL.ARPA>
Tue, 13 Oct 87 21:11:53 EDT

Nic McPhee's essay on anonymity reminded me of an innocent-looking way that names and demographic information are entered into frequently-merged databases: the so-called "warranty registration" cards that come with nearly everything that we buy. What our sex, job, age, and gross annual income have to do with validating the warranty on a TV or a computer escapes me. While government doesn't necessary get ahold of these databases, shady characters in the private sector should have no trouble posing as legitimate businesses and buying these databases.

On a related note, and one not directly related to risks in computers (sorry Peter), the British Government's use of "questionable" means of searching for unlicensed TV receivers may not in fact be a violation of THEIR law or traditions. In many ways, the British system is far less protective of an individual's rights than is ours in the U.S.

Discrimination considered pejorative

Geraint Jones <geraint%prg.oxford.ac.uk@NSS.Cs.Ucl.AC.UK>
Thu, 15 Oct 87 10:04:04 BST

Yes, yes, I too get the annoying annual letter asking me why I haven't got a licence for my non-existent television. I thought everyone did. You can't mean to say that some people have televisions?

Surely the greatest risk of all this information refining is the risk to the ego of the individual who thought he was unique, or at least in an `elite'-sized minority. I mean, I thought I was the only bald, bearded, Methodist, owner of a tandem south of the Trent; what am I going to think when I get the direct-mail advertisment for a hair restorer and a beard trimmer in with my invitation to a tandem rally from the church's home mission division?

Perhaps there is some comfort here for Cliff Jones' original paranoia. He was originally bothered -- RISKS 5.38 -- by the suggestion that he was being marked down as a potential lawbreaker and that someone might carelessly treat that as being the same as having a criminal record. I cannot yet conceive of being in a mechanically-detectable minority small enough for it to be safe to make wild generalisations about us. To be lumped in with a large enough proportion of the population is not to be discriminated against in any new or

unusual way.

There are, for example, one in twenty of us (not 1%, as Ian Batten RISKS 5.42) in the UK without haunted goldfish-bowls in our houses. I forget whether that is 5% of the population, or 5% of households -- we are uncommonly likely to be one- or two- person households, so it is a different proportion. What is depressing is the number of us who seem to be in computer science. gj

---

Pacemakers (Re: RISKS-5.43)

<psivax!woof%psivax@csl.sri.com>
Wed, 14 Oct 87 17:04:29 PDT

In this issue of comp.risks you wrote . . .
>(Peter: Pacemakers DO have serial numbers. I called Medtronic and theirs
>do. I assume other manufacturers also have them in case of recall.)

Why don't you drop us a line if you have questions about pacemakers. I believe we are the only pacemaker company on the net right now. Currently we are about #3 worldwide and growing. We currently have pacemakers with and without serial numbers; they made be read electronically without explanting the pacemaker. In general the trend in the future will be towards such numbers. They are actually most useful for identifying whether we have a problem with our manufacturing process. If we know the serial number of the problem pacer, then we can identify which components when into it, and who worked on it here. (All our pacemakers have serial numbers, but the older one can be read only on the outside of the pacemaker. Our more complicated pacemakers store their number electronically, which can be read by a pacemaker programmer. I work on pacemaker programmers.) --

Hal Schloss Pacesetter Systems Inc., A Siemens Company
{sdcrdcf|ttidca|scgvaxd|nrcvax|jplpro|hoptoad|csun|quad1|harvard|csufres|
bellcore|logico|rdlvax|ihnp4|ashtate}! psivax!woof
ARPA: woof@rdlvax.rdl.com

News Media about hackers and other comments (Re: RISKS-5.43)

Bob English <lcc.bob@CS.UCLA.EDU>
Tue, 13 Oct 87 18:56:11 PDT

> From: Jack Holleran <Holleran@DOCKMASTER.ARPA>
> Subject: News Media about hackers and other comments

> MCI spokeswoman Pamela Small said yesterday[,] thefts that cost the long-
> distance carriers an estimated $500 million in 1986 alone have decreased.

> If "equal access" reduces losses, maybe it's time to invest in those
> companies.

This is a very curious kind of loss. If they stole $500 million dollars in services, the company didn't lose $500 million, unless somehow they

were unable to provide $500 million dollars in service to someone else as a result of the misappropriation of resources. While there would be some of that, I find it very difficult to believe that the real number is even a significant fraction of that. There are other real costs associated with this sort of theft--loss of goodwill by the mischarged party, accounting costs associated with rebalancing the books, etc--but those are probably small as well.

In short, the companies have a vested interest in making their losses appear as large as possible. While they show a paper loss of $500 million to theft, all that was stolen was paper money that will not be replaced if the theft ceases, and their revenues will not increase by an appreciable amount.

Phone theft is not so much an economic problem as a social one. The phone companies pursue the legal aspects of it quite aggressively because they want to prevent it from becoming widespread enough to do actual damage, but they don't take obvious preventative measures to prevent it or detect it earlier. They don't, for example, look for sudden large changes in service levels and flag them as suspicious.

--bob--

P.S. I heard the other day that the average driver commits about 10 traffic violations every mile here in California. I'm looking forward to the day when the CHP can track my car through its computers.

Password bug - It's everywhere.

<To: risks@csl.sri.com>
Thu, 15 Oct 87 15:00 EDT

After reading Geof Cooper's posting on the password truncation problem, I tried it on every Unix machine I could find. Only the first 8 characters counted on any of them. Here's the list:

Machine	Operating System
VAX 750	Ultrix 1.2
VAX 8600	Ultrix 2.0-1
VAX 750	Berkeley 4.3
Celerity 1260D	Accel Unix 3.4.78
IBM RT-PC	AIX 1.2
Sun 3/160	3.0

Looks like this bug has been there for quite some time - maybe since the beginning. Can you spell propagation? Maybe this bug can be used for some copyright infringement suits? I suppose all of the Unix-computer producing companies assumed this part of the code worked and didn't need looking at. My guess is that there are actually few of us who use more than 8 characters anyway, so the implications are not as severe as it might seem, but it

sure decreases the search time. Where might the most serious implications of this be? Unicos machines with classified data? Other defense machines?

-Mike Russell

Re: YAPB (yet another password bug)

Brint Cooper <abc@BRL.ARPA>
Tue, 13 Oct 87 20:57:11 EDT

Geof (no relation) expresses surprise that 4.3 Unix "silently" truncates passwords to 8 characters. Was this a secret? Did not 4.2 and 4.1 do the same? I don't believe that there has been a 14-character password since the days of the PDP-11.

Brint

[More importantly, any algorithmically generated password is easier to crack... In this case, once you know more than one password, you could easily infer the algorithm... With my 7-character name, I get only one free character. The password generating scheme Geof refers to is much dumber than the 8-character truncation. But it is nice to know about the truncation! PGN]

Civil Disobedience (Re: RISKS-5.43)

Scott Dorsey <kludge@pyr.gatech.edu>
Wed, 14 Oct 87 17:52:39 EDT

In Risks Digest 5.43, I find:
>It seems to me that as the computerization of society continues, the idea of
>engaging in civil disobedience via computer is bound to come up more often.
>Some computer CD might resemble ordinary computer crime and sabotage except
>for the motivation of the individuals carrying it out. I've heard folklore
>about politically motivated crackers for years now; do RISKS readers know of
>any actual examples?

I seem to recall a mention that the Berkeley computer center was occupied by protesters sometime in the sixties, who claimed that the computers were being used for war work. A sit-in was staged, as well as the damage of some equipment and a large number of tapes. I don't know precisely if any significant damage was done.

On a slightly more current note, a couple of years back, a student who was upset with the student government policies here at Georgia Tech formed an organization called the Barbecue Liberation Front (the gripe, as I recall, had something to do with a cancelled cookout), which among other things froze the student government accounts, and sent messages to all users each second on one of the undergraduate class machines, making it unusable.

This is as close to political motivation as I have ever seen on

the Tech campus. Although it may be a rather pitiful example, it is as political as anything ever gets in a place where Poly Sci profs refer to the Washington Post as an "anarchist rag."

Scott Dorsey Kaptain_Kludge
SnailMail: ICS Programming Lab, Georgia Tech, Box 36681, Atlanta, Georgia 30332
Internet: kludge@pyr.gatech.edu
uucp: ...!{decvax,hplabs,ihnp4,linus,rutgers,seismo}!gatech!gitpyr!kludge

---

Civil Disobedience (Re: RISKS-5.43)

<bfisher.ES@Xerox.COM>
14 Oct 87 13:19:13 PDT (Wednesday)

Anent Prentiss Riddle's comments on Civil Disobedience - (CD)-- I suggest that 'Civil Recalcitrance' (CR) is already here. This is defined as nonviolent copping out by using the 'computer' as a shield. Two recent examples --(1). Eight weeks for one of the country's largest insurance companies to issue a check for a health insurance claim -- ("I'm sorry - it's in the computer and there's nothing we can (read 'want') do about it; (2). Repeated billing for an item no longer in use and returned to the lessor. (I'm sorry, the rental data base is in a different computer than the return for credit base and they don't talk to each other). The only (simple) way to clear this was to pay the rental data base people for the item, even though the sales data base people had already been paid by return of the item.

Bill Fisher

Computer civil disobedience

<eugene@ames-nas.arpa>
14 Oct 87 10:31:20 PDT (Wed)

Prentiss Riddle brought up the topic of computer civil disobedience. The example of Falwell is an excellent one, and I believe that some organizations have thought about this type of blocking both for offense and defense. First, the organizations that are really worth blocking typically don't have dial-in access. Second, some "good organizations" might be `blocked' by those with differing opinions (creationists blocking science BBSs?). But the real reason I wanted to send you this is to point out that some bureaucratic organizations like the FBI and Service Service take dim views of civil disobedience, partly this is because of their mission.

Recently, a Vietnam Viet lost his legs to a train in an act of civil disobedience at the Concord Naval Weapons Station. All parties agree this is a tragic act. If anyone is going to embark on computer civil disobedience, they had better think about all possible consequences INCLUDING getting shot. The people who work for the SS and FBI may not know computers very well, but computers are increasingly used in criminal capacities. At the time of suspicion, they (their perspective) might not have the time to evaluate, but might run into a building with

guns drawn when there are only teenagers there. The situation for them is something similar to the issue of Toy Guns; it's that WE see the situation from a different perspective. Softwar is a real possibility for these people (even though they may not be aware of it, now).

One of the risks of computers we have not discussed is the "evil" unintended (and non-military) uses of computers. One BBS in the Bay Area (noted as a headline story) was a neo-Nazi BBS. Dan Pasquale of the Fremont PD is most concerned with the BBSs of pedophiles. More likely than not there are neo-Nazis and pedophiles reading RISKs, so "evil" is a minority perspective. The problem becomes discriminating between crime and liberties, disobedence versus threat [sorry, I lost the "real" word].

I don't wish to defend the actions of what I regard as an increasingly police-state mentality of the country (it's largely, "WE" the people who are pushing this BTW), but I do wish to avoid severed legs and teenagers shot by carrying laser tag pistols.

--eugene miya

Phalanx Revisited (Risks to Carrier Aircraft)

Barbarisi <marco@ncsc.ARPA>
Wed, 7 Oct 87 13:34:20 CDT

Are US Navy aviators at risk from Phalanx systems on their own ships? I mention this because I noticed that aircraft carriers have Phalanx guns mounted at the stern of the ships - in a perfect position to shoot at aircraft approaching a carrier for a landing. I noticed this while glancing at a Varian advertisement on page 2 of the Oct. 87 issue of Defense Electronics.

Marco

SSNs

Bill Gunshannon <bill@uunet.uu.net>
5 Oct 87 13:17:57 GMT

From: bill@trotter.usma.edu (Bill Gunshannon)
Organization: US Military Academy, West Point, NY

In response to an article in:
RISKS-LIST: RISKS-FORUM Digest Wenesday, 30 Sept 1987 Volume 5 : Issue 41
>From: P. T. Withington <PTW@YUKON.SCRC.Symbolics.COM>
>Subject: Re: Risks in the Misuse of Databases? [RISKS-5.40]
> All
>this despite existing laws that state SSN's are to be used only for
>social security and not as a identification number.

I think it is time we put this notion to rest once and for all.
How can you say that is the only legal use for the SSN when I was just

required by law to get my daughter (8 yrs old) a SSN and I will have to include that number on MY income tax return from now on. Now, unless they have revoked the child labor laws, she is unlikely to need that number, for Social Security purposes, for at least 9 more years. :-)

bill gunshannon
Martin Marietta Data Systems USMA, Bldg 600, Room 26 West Point, NY 10996
UUCP: {philabs}\ WORK (914)446-7747
{phri } >!trotter.usma.edu!bill
{sunybcs}/

Search RISKS using swish-e

THE RISKS DIGEST

Forum on Risks to the Public in Computers and Related Systems

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

Volume 5: Issue 45

Monday, 19 October 1987

Contents

Stocks into Bondage? Storm prediction? Computer relevance?

Peter G. Neumann <Neumann@KL.SRI.Com>
Mon 19 Oct 87 17:47:09-PDT

With the Dow losing 508 points today (down 22.6% from 2247) and 744 points since the beginning of last week, please be on the lookout for any careful analyses of the extent to which computers were involved in setting off and extenuating the crash -- e.g., computer-programmed selling, rapid responsiveness of the computer systems (despite the delays in the tickers), trying to optimize locally, etc. (No speculations, please.) Certainly, margin calls and the human tendency toward fear and panic in that kind of a crisis contributed to an extremely unstable feedback loop. But let's see if we can identify precisely what roles the computers played, for better or for worse.

Also, I hope one of our European readers will follow up on any further reports that computer systems have been partially blamed for the failure of weather predicters to warn about the once-in-a century hurricane-force storm that blew through England and Western Europe on 16 October 1987. Apparently predicters still did not have a clue even after the winds (which reached up to 110 mph!) had begun. But the home secretary said it would be unfair to blame the forecasters -- the wind shifted suddenly and sped up unexpectedly.

UNIX Passwords

Dave Curry <davy@intrepid.ecn.purdue.edu>
Fri, 16 Oct 87 08:22:19 EST

The truncation of UNIX passwords to 8 characters is not a bug, it's a feature. If you have source, examine the code to libc/gen/crypt.c.

Your password is *not* actually encrypted on UNIX. Rather, it is used as the *key* to encrypt a standard block of text (a block of zeros, although this is irrelevant) using a modified version of the DES algorithm. The result of this encryption is what is usually called your "encrypted password".

The keys for DES are 56 bits long. 8 characters, at 7 bits per character, makes 56 bits. There's no point in using characters after that, since you can't put them into the key.

It seems to me this isn't that serious; if I choose a password you're going to guess easily, chances are the length isn't going to matter -- guesses made on names, birthdates, etc. are not based on length, but based on other criteria. Using a list of about 2000 proper names I have, only 9% of those names are longer than 8 characters. Birthdates (mmddyyyy) are eight characters long. Phone numbers are 7 digits, unless you add area codes (although if you use *your* area code, the cracker now has 3 characters of your password...).

The only thing truncation makes easier is exhaustive search generating passwords like "aaaa", "aaab", "aaac", etc. Even with only 8 characters, that would take a *long* time... (although you could do it on a Cray, I guess). SSNs are 9 characters long, but the number of 9-digit permutations of 10 digits is still small enough to make exhaustive search reasonably trivial.

--Dave

[There were many contributions on this topic. This was the most cogent. PGN]

Let the Punishment Fit the Crime...

Mike McLaughlin <mikemcl@nrl-csr.arpa>
Sat, 17 Oct 87 12:49:00 edt

Recent issues of Risks have mentioned juvenile hackers who perpetrated com-

puter crimes. One youth's computer was destroyed, by court order. A reader felt that was inappropriate. I disagree. It should have a significant deterrent effect.

In the Shenandoah Valley of Virginia there is a judge who orders that convicted poachers' guns be destroyed, and that the poachers watch. When I met the judge (socially!) I suggested that they be sold as confiscated goods rather than being destroyed. He replied that the poachers were emotionally involved with their possessions, and that destruction was far more effective than mere confiscation.

After 14 years of hiking and hunting in his jurisdiction, meeting people who lived in that area, I have to agree with him... and with the judge who ordered the computer destroyed. Perhaps both judges are Gilbert and Sullivan fans.

- Mike McLaughlin

["A more humane Mikado ...:
My object all sublime...
To let the punishment fit the crime ..."

But G&S had something for the computer buff:
"We only suffer to ride on a buffer ..." PGN]

Re: Computers and civil disobedience

James Peterson <peterson@MCC.COM>
Fri, 16 Oct 87 09:02:44 CDT

Prentiss Riddle raises the possibility of using computers for civil disobedience or protest. I remember reading a few months ago about a person who was really upset at one of the fundamentalist religous organizations (Falwell's) and programmed his PC to use its auto-dialer to call their toll-free number, wait 30 seconds, hang up and call again. The article in the paper was because he had been arrested and his equipment confiscated, although it was not clear to me what law he had violated. jim

---

Civil Disobedience

Clif Flynt <ucbcad!ames.UUCP!ihnp4!chinet!clif@ucbvax.Berkeley.EDU>
15 Oct 87 15:39:32 CDT (Thu)

[... Mention of the Falwell case...]

As an aside, and not a risk, to my mind, You might be amused to know that one of the Michigan State Representatives (Perry Bullard) operates a conference on a large computer bulletin board in his district. Along with answering questions from the BBs'ers, he posts the text of various bills he is introducing, and accepts the comments of the readers. On a couple of occasions, I think he modified the bill after reading the reactions of the folks.

At this point, he is selecting for a small segment of the voters he represents, but as more and more households acquire modems, this might make our system more of a democracy than it's been since all the voters in a town could attend one meeting.
Of course, as reading the Net shows, you also get a lot more noise...

Clif Flynt

[And that is not a risk -- it is a certainty. We have noted before in RISKS the dangers of overly instant reaction to events. But there are also denial of service issues, flooding with bogus computer-generated messages all appearing to come from different constituents, flooding with legitimate computer-generated mass mailings sent by special-interest groups, etc. PGN]

Civil Disobedience

<fulk@cs.rochester.edu>
Fri, 16 Oct 87 10:47:01 EDT

I think the notion of civil disobedience needs some clarification:

While the term "civil disobedience" is full of ambiguities, I believe the most common use is to describe _public acts of protest_. Thus the lunch counter sit-ins, the Concord Naval Base protest, the Women's Peace Encampment protests at Romulus, the Berrigan's blood-drenched draft files, draft card burnings, etc. Such acts are carried out after much consideration of the consequences, and are planned to have an impact on public opinion. This is not to say that these acts always take place in a glare of publicity; often it is hoped that a long series of such acts will draw attention and perhaps convince some of the public of the conviction of the protestors.

Computer break-ins and BBS/800 number flooding are normally private actions. If they were performed publicly, they would have little effect of the sort the protestor would like: a hacker pounding away at his computer doesn't make for high drama.

Civil Disobedience

Brent Chapman <chapman%mica.Berkeley.EDU@violet.berkeley.edu>
Fri, 16 Oct 87 00:32:35 PDT

In RISKS-5.44, Scott Dorsey (kludge@pyr.gatech.edu) writes:
> I seem to recall a mention that the Berkeley computer center was
>occupied by protesters sometime in the sixties, who claimed that the
>computers were being used for war work. A sit-in was staged, as well
>as the damage of some equipment and a large number of tapes. I don't
>know precisely if any significant damage was done.

I've been here for a little over three years, and I've always found it curious that, in general, the users here have little or no idea where the machine rooms are. They're not really hidden, but their locations aren't

really advertised, either. I don't know if that's a reaction to what Scott mentioned, or not. To my knowledge, there aren't any "showcase" machine rooms; you know, the "glass cages" we all love to hate...

The EECS building at Berkeley (Cory Hall) has a fancy card-key system to control access to critical areas (machine rooms, labs, and such), and to the building itself after hours, apparently installed after a grad student was injured when he opened a package found lying in a terminal room that turned out to be a bomb. Getting around the system is fairly easy; you just stick your head into the terminal rooms _outside_ the controlled zone and shanghai someone you know who has a card for a few seconds.

The building in which most of the CS division and the Computer Center are located (Evans Hall, along with the Math Dept., Stat Dept., and several others) is also supposedly locked up after hours. It doesn't have a card-key system like Cory; they just lock things up. In theory, you can get to the terminal and printer rooms in the basement, but not to the rest of the building. In practice, once you get to the basement, you can get to the rest of the building.

At Stanford, on the other hand, in order to get to the comp center staff offices, you have to go _through_ the machine room -- the door is wide open.

I don't know how much of this is "justified", and how much of it is just bureaucratic paranoia. How "secure" are other academic and commercial comp centers? Is Berkeley the only campus to try the "security through obscurity" approach, rather than showcasing their toys? Have there been any cases of terrorist or political attacks on comp centers? We're all used to considering the electronic access considerations of computer security (networks, dialups, etc.) here; how about the physical considerations? How many of you have no idea where the machines you use are physically located? How many of you don't even know exactly what type of machine you use (for example, is your VAX a 750, a 780, or a 785?)? Is the unawareness of the details of the underlying hardware becoming more or less prevalent, and is that good or bad?

This should give us all some food for thought...

Brent Chapman Senior Programmer/Analyst
koala!brent@lll-tis.arpa Capital Market Technology, Inc.
lll-tis!koala!brent 1995 University Ave., Suite 390
Phone: 415/540-6400 Berkeley, CA 94704

[I remember in the early 70s that the MIT computer center facilities had restricted access to the machine room via a spiral staircase to the next higher floor -- except that the emergency exit was unalarmed and sometimes left ajar. PGN]

Unemployment Insurance Cheaters

William Smith <wsmith@m.cs.uiuc.edu>
Sun, 18 Oct 87 21:29:00 CDT

I heard on a TV news report of a computer matching between employees of one company in Indianapolis, Indiana and a list of unemployment check recipients. A number of overlaps were found last week [Oct 17] who will be prosecuted.

<I couldn't find any references in the newspapers I had available this weekend in Fort Wayne. Does any one have more definite information? -- Bill Smith>

Computer Services as Property (Re: RISKS-5.41)

Doug Landauer <landauer@Sun.COM>
Tue, 6 Oct 87 13:07:18 PDT

> From: "Arthur_Axelrod.WBST128"@Xerox.COM
> I think we all agree with the fundamental premise, i.e. that information
> is a form of property and is entitled to the same protection as any
> other form of property.

Absolutely *NOT*!!! I know of no one who thinks (e.g.) that their house, their car, their wallet and their Unix files (or their IBM-PC software) are entitled to *the same* protection.

The significant difference between information and "real" property is that if you steal real property, your victim is denied access to that property; whereas if you "steal" information, your victim still has hir copy of it, and may not even notice the "theft". That is why the word "steal" is no longer appropriate in this context.

What *I* think many of us agree on (except R.M.Stallman, of course) is that information is a form of property and is entitled to *some* protection. What our linguistic, ethical and legal systems have not yet come to cope with is just what sort of protection information is entitled to, and what sort is feasible.

Doug Landauer Sun Microsystems, Inc.
ARPA Internet: landauer@sun.com Software Products Division
UUCP: {amdahl, decwrl, hplabs, seismo, ...}!sun!landauer

Successor to Sun Spots

K. Richard Magill <umix!oxtrap!rich@uunet.UU.NET>
Fri, 16 Oct 87 13:10:15 edt

My new explanation why computers sometimes do random unexplicable things. (replacing my previous, "sun spots").

[about the first sentient system] ... and she amused herself by planning, and sometimes carrying out, malicious computer failures and data losses in order to watch the humans flail about helplessly like

ants around a crumpled hill.

-- Orson Scott Card from "Speaker for the Dead"

Search RISKS using swish-e

THE RISKS DIGEST

Forum on Risks to the Public in Computers and Related Systems

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

Volume 5: Issue 46

Wednesday, 21 October 1987

Contents

Portfolio Insurance and Wall Street's meltdown

Rodney Hoffman <Hoffman.es@Xerox.COM>
21 Oct 87 15:53:15 PDT (Wednesday)

Excerpted from the 'Los Angeles Times', Tuesday, Oct. 20, 1987:

PORTFOLIO INSURANCE MAY HAVE WORSENED SELLOFF, TRADERS SAY
By Michael A. Hiltzik

In December, 1986, New York Stock Exchange Chairman John J. Phelan warned a

Washington audience that a new form of computerized stock and futures trading known as portfolio insurance could someday lead to "financial meltdown."

The markets laughed him off.... [T]here are strong indications that computerized portfolio insurance programs inspired the snowballing waves of selling during the market's catastrophic collapse. The impact of portfolio insurance programs on the market's epic fall Monday and last week cannot be precisely gauged. But estimates place the amount of assets "protected" by the programs ... at as much as $61 billion.

Because of the mechanics of portfolio insurance, a significant portion of that pool of cash was poised before last week to begin marching, all at once, in a single direction: down.... [T]he leading insurance technique involves selling not stocks, but related stock-index futures, and using the porceeds to offset stock losses. As the selling waves hit the futures markets, they drive futures prices down, which in turn drag stock prices down....

Even people who sell portfolio insurance acknowledged that the technique is probably a leading villain of the market collapse -- and what's more, failed to protect clients from the lossses they thought they would avoid. Portfolio insurance firms all use somewhat different computer models to dictate trading for clients; some were apparently more successful than others in protecting clients from losses this week and last week. But all showed they had devastating shortcomings, [Preston W. Estep, head of a leading portfolio insurance firm] said....

[discussion of the past warnings and fears about the growing interrelationship between future and stock markets]

Program traders... have often been blamed for exacerbating the sharp stock price moves of the last few years because their computer programs are designed to order the sale or purchase of millions of dollars of stocks in the blink of an eye. Portfolio insurers add another bias to that system: one that encourages sharp downturns.

[detailed discussion of one scheme: "dynamic hedging" developed by University of California, Berkeley business professors Hayne Leland and Mark Rubenstein]

More important than clients' individual losses, however, is the way portfolio insurance tends to magnify market slumps. Because the clients' concerted selling forces futures prices down, that attracts investors who strive to make money from the difference in price between the futures and their related stocks. In roughly simultaneous transactions, they buy the futures and sell the corresponding stocks. In turn, that forces stock prices further down, which kicks in more insurance-related sales in the futures markets, and so on.

Software firms put on guard by Act

<bowen%prg.oxford.ac.uk@NSS.Cs.Ucl.AC.UK>

Wed, 21 Oct 87 15:55:02 BST

From the Times, London, 20th October 1987:

Computer Horizons, Jobscene, by Darrell Ince,
Prof of Computer Science, Open University, UK.

`The new Consumer Protection Act, which comes into force next year, could provide a number of headaches for British software developers. At the same time, it is also likely to result in an increase in both job opportunities and salaries for one neglected area of software engineering -- quality assurance.

Until the new law takes effect anybody who is injured because of an error in a software product has to carry out the difficult process of establishing fault on the part of the company which supplied the product.

Once it comes into force all that will be required is to establish a casual link between the injury suffered and a defect in the software product.

This puts immense pressure on software companies to make sure that their software is correct. ...

[The article goes on to mention the techniques which quality assurance specialists can use including...] one American concept...the Black Team. This is a collection of hackers whose function is to try and make a completed software system crash.

[Prof Ince suggests that...] ...the bulk of companies...still take a relatively relaxed view of software quality.

The new law will change this, and, if as expected, companies start becoming directly liable for software products, then there should be a massive expansion which, initially, may not be meet be current levels of staffing. ...

[The article concludes] ...I think we can all excuse current software quality practitioners their broad grin as they read the newspaper accounts of the problems that British software houses will face over the next three years.'

Any comments? [Had any jobscene phone calls lately? PGN]

World Series Phone Snafu [Telephones Whirled Serious in Fall Classic]

<TMPLee@DOCKMASTER.ARPA>
Mon, 19 Oct 87 02:26 EDT

I don't know how it played in the national media, if at all, but the telephone systems in the five midwestern states surrounding Minneapolis/St. Paul were essentially thrown continuous strikes for three hours yesterday (Saturday) morning.

After some minor skirmishes in the lines where the local tickets (i.e., non series ticket holders, non-bigwigs, etc.) for the first two games of the World Series had been sold earlier in the week, the sole ticket franchisee (one of the local major department store chains) decided to make things more pleasant by selling the 10,000 local tickets for games six and seven by taking orders over the phone. The number to call, which was staffed by 35 operators, was announced at 0755AM Saturday on the local television and radio stations, some of which cover a good part of five states (North and South Dakota, Wisconsin, Iowa, and Minnesota.) 200,000 calls an hour were attempted to that number until the last ticket was sold at about 11:00 AM. Most phone exchanges in the area were for all practical purposes shut down by the overload.

The news reports weren't very specific about how bad the delays were where, but did mention that the effects were spread over the five-state area. I was unable to get a dial tone during the entire period. 911 service was useless -- the 911 equipment of course was all right -- if one could have gotten a dial tone in any reasonable time. It was reported that one suburb realized the danger quickly and stationed its fire trucks at strategic intersections just in case and police departments broadcast a note requesting people with problems to drive to the nearest precinct rather than try to call. It was very fortunate that apparently there were no emergencies -- the only incident reported was that someone had discovered that a relative had died and tried to call for help on 911; in that case a rapid response would not have mattered. And there was also the poor fellow in Rochester, Mn., (area code 507) who happened to have the same number as the ticket line (area 612) -- and was waiting for calls in response to a newspaper ad to sell some of his belongings before he left for college that afternoon. He was not amused.

The ticket people said they'll have to come up with a third game plan next year. (Of course they'll need it!)

Re: Civil Disobedience (RISKS-5.45)

<sdcsvax!ames!elroy!mss!jpj@ucbvax.Berkeley.EDU>
Wed, 21 Oct 87 10:00:08 PDT

A computer system being used to flood a BBS with calls is *NOT* civil disobedience - it is an act of terrorism. Civil disobedience is an effort to *increase* dialog - to make people aware of a specific concern. It is typically undertaken at some risk to the participants (either physical, legal or both), as recent events have dramatically demonstrated. It is in the highest traditions of democracy and this nation's history.

Flooding a BBS, on the other hand, is an act designed to inhibit dialog. It is meant to intimidate and debilitate other participants in the debate of public policy. Ultimately this is an act of cowardice and not worthy of being justified as "civil disobedience."

Jim Jenal (aka ...!scgvaxd!mss!jpj)

Mayfield Senior School (" ...!ihnp4!mss!jpj)

Destruction of confiscated computers

"Lindsay F. Marshall" <lindsay%kelpie.newcastle.ac.uk@NSS.Cs.Ucl.AC.UK>
Wed, 21 Oct 87 15:14:20 BST

Mike McLaughlin (RISKS 5.45) suggests that destruction of confiscated computers should have a significant deterrent effect and cites poachers in Virginia. He perhaps should look at the history of Moonshining in that area (or in any other area/country that you care to name). The destruction of the "tools of the trade" has NEVER deterred them - moonshiners are famous for coming out of court, straight into the hardware shop and buying the materials for new stills. I dont see why poachers should be any different nor hackers - let's face it probably doesnt cost that much to replace the sort of computers they are using (at least in the US anyway). I accept that SOME people MAY have strong emotional ties to particular pieces of equipment, but its destruction is more likely to make these people think of revenge than anything else. Let's face it Judges aren't famous for their knowledge of human psychology (OK neither are computer scientists....). What was it Reagan said about Social Science degrees and the jurisdiction??

Lindsay

Weather Forecasts

"Lindsay F. Marshall" <lindsay%kelpie.newcastle.ac.uk@NSS.Cs.Ucl.AC.UK>
Wed, 21 Oct 87 14:52:22 BST

There have been a variety of stories about weather forecasting and the recent bad weather. The gist of these seems to be (sorry about hazy details...) :-

1) The system based on a Cyber (the Met office?) failed to predict the storm.

2) A system based on a Cray DID predict the storm.

3) Le Monde carried a correct forecast on WEDNESDAY!

4) The bad predictions have been attributed to a lack of upper air measurements, satellite data not being particularly useful in this case.

5) Old Moore's Almanac said that there would be storms in October.

6) It's God's revenge on the Thatcherite Yuppies.....

Lindsay

Anonymity and high-tech: indirection (Re: RISKS DIGEST 5.43)

Robert Stanley <roberts%cognos%math.waterloo.edu@RELAY.CS.NET>
19 Oct 87 17:25:53 GMT

In risks 5.43 Nic McPhee introduced anonymity as the best protection:
>From: mcphee@ratliff.cs.utexas.edu (Nic McPhee)
> One of the greatest guarantees of privacy is anonymity.

This hits right to the heart of the matter, and the question remains one of how to preserve anonymity in an age of increasingly sophisticated, tireless, and undistractable records searchers. The common property of all answers to this question is that it requires effort: anonymity is no longer available by default, but that does not mean that it is unavailable.

There are three strong (high probability of success) approaches to achieving electronic anonymity:

1. Thoroughly understand the legal position and fight for your rights;

2. Use cut-offs that break the search chain; and,

3. Generate the crowd in which to hide.

This forum has discussed legality quite extensively. There are plenty of mechanisms available for finding out and getting changed or deleted information that is held on file about you. You can also do a lot to ensure that there are as few direct pointers (common ID's like social security number) as possible. The drawback of this approach is that it attracts the attention of the beureaucracy, which may lead to more trouble than the protection is worth, and further lays you open to trojan horse attacks by people who obtain access (legal or otherwise) to government files which contain information on you.

However, as an example, I was once extremely paranoid about having my private life analysed when automated mailing lists started to appear. I therefore kept a precise record of EVERY occasion when I released certain information in writing (I always refused to give details over the phone) and carefully inserted one variant as a key in each case. If a particular variant started appearing from another source it was 100% certain that the information had been propagated, and I would go directly (and angrily) back to the original recipient of the information and demand an explanation. This achieved the desired effect until proliferation led to corruption, and the trace keys became hard to devise with sufficient robustness to guarantee their survival across compressed address lines and so on. Of course, I may have become an entrant on a blacklist of some kind, but I don't think THEY were sufficiently organized. What I did find was that a letter to the wife of the president at home (amazing how easy that sort of info was to discover :-)) with copies to the president plus the relevant department at work guaranteed attention. Firm contention that one understood how computer systems work, and discussion of operator liability usually resulted in speedy remedial action. But this takes hard work.

At the other end of the scale, simple cut-offs to break chains work wonders. There is very definitely no direct link between roberts@cognos.uucp and, for instance, the residential address of Robert Stanley, private citizen. All my junk mail, including credit cards, subscriptions, and so on, goes via an

address of convenience. (by the way, should you crack Cognos' personnel database, you will find a correspondence rather than a residential address, but a telephone number for a telephone that does ring at my home). A PO box is the simplest, and Canada Post at least limits the connection between a PO Box and an actual person to a single local post office ledger entry. The only positive link they require is a telephone number, which could be at work. Next best is to use a service agency, and you'd be surprised at how cheap and convenient they can be. In fact, your worst danger is from your real friends, who may have your personal information thoughtfully recorded among their own records. Most of us don't tend to keep these encrypted. Yes, the memory telephone is a lethal instrument, as is the last number redial facility.

Finally, it is possible to create your own haystack, by making the information explosion work to your advantage. Get on every kind of list you can, at every opportunity. When faced with too much information, particularly contradictory information, systems and people alike usually decide to ignore the case in favour of an easier one. You can just see the evidence for the prosecution against a TV license non-payer including letters of application for game-show appearance, when in fact you are one of the 1% TV non-owners! Innocent until proven guilty does still apply.

Robert Stanley, Cognos Incorporated, P.O. Box 9707, 3755 Riverside Drive,
Ottawa, Ontario CANADA K1G 3Z4 Phone: (613) 738-1440
uucp: decvax!utzoo!dciem!nrcaer!cognos!roberts

Berkeley's computer security

<forags@violet.Berkeley.EDU>
Tue, 20 Oct 87 09:01:05 PDT

When Berkeley's computer center was occupied in the early 1970's, the only thing which saved us from major damage was ignorance. Damage (which was not severe as I recall) was concentrated on tape drives and other things with moving parts. One of the operators told me that if he had been sympathetic to the demonstrators, he would have directed them to the innocuous box which held the CDC 6400's mainframe.

Al Stangenberger, Forestry, U.C. Berkeley

Berkeley's computer security

David Redell <redell@src.dec.com>
Tue, 20 Oct 87 11:57:03 PDT

A little more history of machine room physical security at Berkeley,
as raised by Dorsey (RISKS-5.44) and Chapman (RISKS-5.45):

> "I don't know if that's a reaction to [the sit-in that] Scott
> mentioned, or not"

At the time of the anti-war sit-ins, the computer center machine room

was in the basement of the old math building, and had no physical security to speak of. Users would submit jobs by walking into the machine room and placing their card decks on a counter that was about six feet from the twin CDC 6400 mainframes. When the demonstrators tried to get in, physical security consisted of a burly operator trying to hold the door closed!

Independent of any actual damage done during the demonstrations (very slight, as I recall), the computer center management virtually freaked out about their vulnerability. The machine room in the new math building was already more secure -- for example, card decks were submitted in a separate room and handed via a small pass-through into the machine room -- but they looked very hard for other risks. One wall of the new room had large observation windows of thick reinforced glass; they decided even that was too risky, so the hallway outside the windows was closed to the public. Access by computer center staff became much more controlled, and machine room tours were curtailed. Of course, by the time these and other measures were in place, the demonstrations were pretty much a thing of the past, but it's an interesting example of how a tough security policy often results from an earlier flimsy one plus a bit of scary experience.

Dave Redell

Computer Services as Property

<Rick.Busdiecker@H.GP.CS.CMU.EDU>
20 Oct 1987 08:10-EDT

> Date: Tue, 6 Oct 87 13:07:18 PDT
> From: landauer@Sun.COM (Doug Landauer)
>
> What *I* think many of us agree on (except R.M.Stallman, of course) is that information is a form of property and is entitled to *some* protection.

I think that this is a somewhat inaccurate characterization for a couple of reasons. Firstly, RMS appears to be quite concerned that the informational property rights of others are not violated, although it could certainly be argued that hir motives are of the CYA variety. Secondly, e goes to great lengths to explicitly spell out the protection of GNU project software. If e didn't feel a need for any protection, the software could simply be placed in the public domain.

Rick

<<PRITCHAR%CUA.BITNET@wiscvm.wisc.edu<>
Tue, 20 Oct 87 16:28 EDT

(Hugh Pritchard -- CUA Systems Programming)

Subject: Information as property
To: RISKS@SRI.COM

> From: landauer@Sun.COM (Doug Landauer)
> > From: "Arthur_Axelrod.WBST128"@Xerox.COM
> > I think we all agree with the fundamental premise, i.e. that information
> > is a form of property...
> Absolutely *NOT*!!! I know of no one who thinks (e.g.) that their
> house, their car, their wallet and their Unix files (or their IBM-PC
> software) are entitled to *the same* protection.

Information purveyors do.

> The significant difference between information and "real" property is
> that if you steal real property, your victim is denied access to that
> property; whereas if you "steal" information, your victim still has hir
> copy of it, and may not even notice the "theft".

Information certainly does have value. And that value is altered when the information is spread around, whether the originator retains a copy or not. Ask any spy. And what makes 'sharing' information more defensible than stealing it? Want to share your lover/spouse with me?

BTW, I think the legal term 'real property' refers specifically to land and improvements thereto, like houses. All other forms of property are personal property.

> What our linguistic, ethical and legal systems have not yet come to
> cope with is just what sort of protection information is entitled to,
> and what sort is feasible.

How long have copyright, trademark, and patent laws been in existance? I'm not claiming that these laws remain the most appropriate means of redress, but only that the concept of protecting information and other 'copyable' property is hardly new.

Hugh Pritchard, Systems Programming, The Catholic University of America, Computer Center, Washington, DC 20064 USA, (202) 635-5373
Disclaimer: My views aren't necessarily those of the Pope.

Search RISKS using swish-e

THE RISKS DIGEST

Forum on Risks to the Public in Computers and Related Systems

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

Volume 5: Issue 47

Thursday, 22 October 1987

Contents

Programmed Trading and the Stock Market Decline

"LT Scott A. Norton, USN" <4526P%NAVPGS.BITNET@wiscvm.wisc.edu>
Thu, 22 Oct 87 00:34:10 PDT

An interview on this afternoon's (21 Oct 87) "All Things Considered" with an investment expert named Thomas Tisch [sp?] discussed the impact that programmed stock trading had on last Monday's stock market losses.

According to Mr. Tisch, aggressive programmed trading typically is an attempt to take advantage of a difference in prices between different offerings of the same stock. For example, analysts will compare the price of a group of stocks on the NY Stock Exchange with the price of an option on the same stocks on the Chicago exchange. If a sufficiently large disparity

exists, the programmed sales will be activated, buying the lower priced package and simultaneously selling the higher priced package. Because the disparities in price are usually small, this strategy requires large purchases, on the order of $25 million. During Monday's decline, trading on index futures was suspended, reducing the impact of this form of programmed trading on the market.

In the case of Monday's fall, Mr. Tisch felt that a lot of the volatility the market showed was caused by another kind of programmed trading. Many large institutional investors, such as insurance companies, pension funds, and university endowments, had tried to protect their assets with "portfolio insurance."

To protect against their assets being wiped out, these investors had programmed in a bail-out if their portfolio's value dropped too far. This resulted in an automated panic once the market as a whole started to drop.

[I didn't tape previous the broadcast, so I can't give you Mr. Tisch's credentials. All I have is hastily scribbled notes I took during the interview. I did, though get the following item on tape]

On Tuesday, during an address to the National Press Club, Garrison Keillor was asked what effect the market's decline would have on Bob's Bank in Lake Woebegone. Keillor replied,

> "I think the terrifying thing about this stock market crash is the idea that this could all be going on between computers with human beings hardly involved at all. That these vast banks of computers all over the country, using the phone lines, are battling each other for stocks, and that we have no part in this."

LT Scott A. Norton, USN | From Internet, if you need a gateway, use
Naval Postgraduate School | 4526p%navpgs.bitnet@jade.berkley.edu
Monterey, CA 93943-5018 | or 4526p%navpgs.bitnet@ucscc.ucsc.edu
4526P@NavPGS.BITNET | The WISCVM gateway will close 15 Dec 87.)

Overload closes Pacific Stock Exchange computers, and other sagas

Peter G. Neumann <Neumann@KL.SRI.Com>
Thu 22 Oct 87 17:49:07-PDT

On Monday, a number of NASDAQ market makers abandoned their posts while stockholders were trying to bail out. (A good thing? Don't let 'em sell until it goes up again?) Although this was not a computer-caused problem, it kept the computers from handling the relevant trading during the 508-point drop.

On Tuesday, computerized trading in stock-index futures and options was temporarily suspended for the first time in history in New York, Chicago, and Kansas City.

On Wednesday, the PSE had to shut down its computerized trading system (SCOREX) for about five hours yesterday due to intolerable transmission delays resulting from the avalanche of orders. This was its first complete shutdown since installation in 1979. Volume dropped significantly. (On Monday SCOREX trading was halted in about 5% of the options, due to "technical problems".)

[Source: San Francisco Chronicle, 22 October 1987]

When a brokerage house loses out on transactions it was not able to make, this is what is known as an ERROR OF COMMISSION!

BankAmerica Aides Quit; Sources Cite Data System

Jerome H. Saltzer <Saltzer@ATHENA.MIT.EDU>
Thu, 22 Oct 87 08:57:29 EDT

This morning's (Thursday, October 22) Wall Street Journal, Eastern Edition page 44, contains an article with the above headline, which continues:

"Two top BankAmerica Corp. executives quit after being asked to resign . . . in an action related to data processing problems that cost the company an estimated $25 Million.

"The two men were held responsible . . . for problems in converting to a new computerized accounting system for the bank's trust department last March.

". . . A bank spokesman said the conversion to a new system, called MasterNet, disrupted data processing records to the extent that BankAmerica is frequently unable to produce or deliver customer statements on a timely basis."

The good (?) news is that ". . .the spokesman said . . . 'to the best of our knowledge, no customer information has been lost. . .'"

Jerry

Air Force explores SDI-like technology

Walt Thode <thode@nprdc.arpa>
21 October 1987 1426-PDT (Wednesday)

From the Federal Computer Week (10/19/87) (excerpted, without permission):

The Air Force has issued technology assessment contracts to four teams to explore deployment of a multibillion-dollar Air Defense Initiative that could rival SDI for cost, complexity, and possibly for political debate.

Issued by the Air Force Electronics Systems Division, the contracts, though slightly less than $1 million each, signal the beginning of a major tri-service effort to protect North America from attack by Soviet bombers or cruise missiles.

A central impetus for the ADI research is the effect SDI will have on Soviet strategic planning, according to Air Force officials. The Air Force operates on the assumption that the ongoing progress on SDI has already pushed the Soviets to improve their bomber and cruise missile forces. If this improvement continues, the US will need to deploy ADI even if the threat it is designed to counter is an indirect result of SDI.

The ADI system will bear more than a casual resemblance to SDI, according to Pentagon officials. Like SDI, it probably will include numerous space-based sensing platforms, which can see the entire North American continent and which can control air, ground, and space-based interceptors or hypersonic aircraft. ADI will require a complex real-time computerized command and control system to monitor threats coming from every compass quadrant. Like SDI, ADI's command and control system will have to be able to assess these multiple threats and then control widely dispersed defensive systems...

John Pike of the Federation of American Scientists, a long-time critic of SDI, said the command and control problems of ADI will be even more complex than SDI. "Airplanes tend to blend into the background, especially when they are flying only a few hundred feet above the ground ... The Soviets are obviously going to have their missiles coming in from the north, but airplanes could come in from any direction." ... Former Defense Secretary James Schlesinger estimated that total costs for ADI could run as high as $50 billion.

(The rest of the article discussed contractors/subcontractors and some of the suggestions for methods and timing. One interesting item was the suggestion that airships (lighter than air) are a possible sensor platform alternative.)

--Walt Thode (thode@nprdc.arpa)

Who knows where the computer is?

Graeme Hirst <gh%ai.toronto.edu@RELAY.CS.NET>
Wed, 21 Oct 87 12:49:16 EDT

In RISKS-5.44, Scott Dorsey (kludge@pyr.gatech.edu) writes:
> I seem to recall a mention that the Berkeley computer center was
>occupied by protesters sometime in the sixties, ...

I attended Monash University, Melbourne, Australia, in the 1970s at the height of the student rebellions. The Computer Centre, fearing an imitation of events in the U.S., posted large notices on the doors of the machine room alleging that after the fire alarm bells went off, you had 45 seconds to clear the room before the carbon dioxide came in, the oxygen disappeared, and those remaining died. (This was before the advent of Halon.) It was assumed that the operators were expected to trigger the fire alarm at any sign of a student invasion, though the administration denied this.

In RISKS-5.45, Brent Chapman (koala!brent@lll-tis.arpa) writes:

>Have there been any cases of terrorist or political attacks on comp centers?

Perhaps someone who was there at the time can tell us about the most famous computer centre trashing, that at Sir George Williams in Montreal.

>How many of you have no idea where the machines you use are physically located

In teaching first year, I always make a point of telling the students what the machine is, where it is, and telling them to have a look at it (through the glass). Reason: I want them to have a mental image of the machine, and to understand clearly that the terminal is not the computer.

This is less important than it used to be, but it is still a good idea; many of our freshmen are still complete computer novices (though no longer the majority). Also, knowing the name, power, ability, etc., of many machines will be important for some of the students later on, if they become systems programmers or administrators. It's never too early to start learning that the old ones are Vaxes, the new ones are Suns, the 3/280 is about three times as powerful as the Vax, etc.

\\\\ Graeme Hirst University of Toronto Computer Science Department
//// utcsri!utai!gh / gh@ai.toronto.edu / 416-978-8747

Anonymity

Fred Baube <fbaube@note.nsf.gov>
Thu, 22 Oct 87 10:20:07 -0400

> > One of the greatest guarantees of privacy is anonymity.

The Social Security number is a standard item on many forms where it has no business being. If you find yourself in a situation where they want to know it and they won't settle for not having it, it might be better to switch than fight .. make one up.
Disclaimer: not recommended for interest-bearing accounts and other income-generators, or for giving blood.

[...]

I'm not sure about the current state of affairs here in the States, but about three years ago a fellow in Buffalo was being harassed by the Postal Service for setting up just such a service, where people could get a PO box under a pseudonym. Their excuse was the need to prevent mail fraud, which he said he would always co-operate in the investigation of. For every box the Postal Service wanted to see a real name and a real occupation. When mail pseudonyms are outlawed, only outlaws will have mail pseudonyms.

P.S. I presume the Internet has a rule against anonymous messages.

Re: UNIX Passwords

Richard Outerbridge <outer%csri.toronto.edu@RELAY.CS.NET>
Thu, 22 Oct 87 00:16:39 EDT

The eight character limit may have been designed in, but direct mapping into DES keys is no feature. The average entropy of English is about one bit per letter over blocks of eight or more letters; so rather than 56 bits of equivocation the routine assuredly provides eight. Hashing long strings together using CBC or CFB message authentication techniques yields eight byte hex strings in which every last trace of equivocation is present in a 'random' looking pattern. Time for a change of password routines.

CD vs ADP security

Barry Nelson <bnelson@ccb.bbn.com>
Thu, 22 Oct 87 09:21:34 EDT

In RISKS 5.45 (Brent Chapman, Re: Civil Disobedience), several minimal computer physical security mechanisms were listed.

Although it may be slightly dated, I have found the FIPS-PUB-31 (Guidelines For Automated Data Processing Physical Security and Risk Management,NBS,1974, 95 pp) to be a good basic reference for the issues needing consideration, including: security analysis, natural disasters, supporting utilities, system reliability, physical protection, internal controls, off-site facilities, contingency planning, security awareness, and internal audit.

Of course, there are more recent texts dealing with the same topic, but this is one of the more complete ones I've seen that focuses on computer facilities, control and contingencies.

It is axiomatic that organizations will supply only that security that is (a) affordable and (b) justifiable under the circumstances. Someone must take the responsibility to identify the various options available and evaluate the local risks, making a final recommendation to the top management.

"This document contains statements of opinion by the author which are not attributable to BBN Communications Corporation or its management."

Barry C. Nelson /Senior Systems Engineer /
BBN Communications Corporation / 70 Fawcett Street, Cambridge, MA 02238

Civil Disobedience and Computers (Re: RISKS-5.44)

Robert Stanley <roberts%cognos%math.waterloo.edu@RELAY.CS.NET>
20 Oct 87 16:23:38 GMT

A very interesting fictional treatment of Civil Disobedience in a terminally automated society is to be found in John Brunner's novel "The Shockwave Rider" which has achieved the status of a minor classic in the science fiction world.

Some very telling points are made, and the subject is explored in considerable depth. However, it also points up the fact that the distinction between CD and criminal activity is not so much a point of law, as the degree of fear/anger triggered in the targetted beureaucracy, which usually has sufficient dollars to overwhelm all but the most visible of protestants.

Robert Stanley Cognos Incorporated S-mail: P.O. Box 9707
Voice: (613) 738-1440 (Research: there are 2!) 3755 Riverside Drive
FAX: (613) 738-0002 Compuserve: 76174,3024 Ottawa, Ontario
uucp: decvax!utzoo!dciem!nrcaer!cognos!roberts CANADA K1G 3Z4

Search RISKS using swish-e

THE RISKS DIGEST

Forum on Risks to the Public in Computers and Related Systems

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

Volume 5: Issue 48

Friday, 23 October 1987

Contents

Freak winds in southern England

<bowen%prg.oxford.ac.uk@NSS.Cs.Ucl.AC.UK>
Fri, 23 Oct 87 18:06:00 BST

From front page of "Computer News", 22 October:

``The Metorological Office will look at the performance of its Control Data Cyber 205 supercomputer as part of its investigation following last week's hurricane-force winds. The office has been criticised for failing to predict the speed and path of the storm.

A spokesman for the Metorological Office said that the equipment, including computers, was always under consideration. He added: "The

> Cyber is not an easy machine to work with but all computers are
> fallible." Control Data did not comment.
>
> The Reading-based [southern England] European Centre for Medium Range
> Weather Forecasting, which supplies longer range data directly to the
> Bracknell centre [Met Office, close by], is happy with its Cray X-MP 48
> machine. "We originally had a Cray-1 before upgrading to an MP 22 and MP 48
> and we are exceedingly happy with our machine. "It gets better and better,"
> said a spokesman.''

My understanding is the main reasons for lack of success in predicting the winds were a) lack of data (the storm came from over the sea -- fairly normal in Britain! -- where there are few weather stations) and b) lack of computing power (and lack of good algorithms?).

It has been reported in Britain that (mainland) Europeans were warned not to come to Britain up to 36 hours before the storm (presumably by forecasts from the European Centre mentioned above). It was not made clear as to whether storms were predicted in the English Channel or actually in England. The storm unexpectedly changed direction and increased in ferocity when it struck England.

The BBC TV weather forecast (which uses the Met Office) the night before mentioned than someone had rung up to say they had heard a hurricane was heading in our direction, but the weather forecaster assured us it was not. The storm WAS predicted by the Met Office a few hours before it struck, but most people were in bed by this time. England being rather parochial, most radio and TV stations shut up shop at night. Had it occurred during the day, then storm warnings would have been broadcasted.

Jonathan Bowen, Programming Research Group, Oxford University

---

Computer Weather Forecasting

Robert Stroud <robert%cheviot.newcastle.ac.uk@NSS.Cs.Ucl.AC.UK>
Fri, 23 Oct 87 15:11:56 +0100

The following letter was published in The Independent on Wednesday 21 October. It comes from Norman Lynagh who is the managing director of Noble Denton Weather Services. I have no idea whether he is offically associated with the Meteorological Office but his letter seems to be a clear and accurate statement of what went wrong with the forecasting of last weeks gales. It also contains some interesting insights into the state-of-the-art in weather forecasting. The bottom-line seems to be the familiar GIGO.

Robert Stroud, Computing Laboratory, University of Newcastle upon Tyne
ARPA robert%cheviot.newcastle@cs.ucl.ac.uk UUCP ..!ukc!cheviot!robert

* * * * * * * * * * * * * * * *

Reproduced without permission from The Independent, Wednesday 21 Oct 87, p. 19

Dear Sir,

The Met Office has come under a great deal of criticism as a result of its failure to predict the severe storm in SE England last Friday morning. Some of what has been said is accurate but a great deal has been unfair criticism.

Despite what has been said by many people, it was not until about 8pm that it was really apparent that something out of the ordinary was developing. Even at that stage it was not at all certain that exceptionally strong winds would hit SE England. It was only an increasing threat. By about 11pm it was certain that a storm of unusual severity would hit the SE.

There have been reports from various sources that warning had been given by other meteorological services several days before the event. This is only half true and, in any case, the Met Office was one organisation which did give such a warning.

Several of the most powerful meteorological computers, including those at the Met Office in Bracknell and the European Centre for Medium Range Weather Forecasting at Reading, predicted five days in advance that there would be a major storm somewhere in the region of southern England or northern France towards the weekend. In broadscale terms, this prediction continued each day after that, but the state-of-the-art in weather forecasting is such that it was impossible to predict in any detail either the severity of the storm or precisely when it would strike.

The depression which caused the storm had existed for several days before it struck in SE England. Indeed, it was giving force 11 winds NE of the Azores two to three days earlier. However, during last Thursday, as it moved quickly NE into the Bay of Biscay, the structure of the depression was far from clear. As Murphy's Law always seems to dictate in such situations, there were very few observations available in the vicinity of the depression and it was very uncertain as to what was exactly happening in Biscay.

As mentioned earlier, it was not until Thursday evening that the situation became clear and it became obvious that the SE was going to have a night to remember.

Meteorology now uses the most powerful non-military computers in existence but the advances in the quality and quantity of input data have not kept up with the computer technology. No matter how good the computer and the software, it will not do a very good job if it is given inaccurate input data.

Summarising all the above, I do not think the Met office can be blamed for failing to give a day or two's warning of a once-in-a-lifetime event.

The state-of-the-art of weather forecasting is such that the way this storm developed and the precise detail of its effects could not be forecast more than a few hours in advance.

What is more open to close scrutiny is why warnings to the public were not issued until after midnight. I think they could well have been issued three

or four hours earlier but that is with the benefit of hindsight and it is really a question which only the Met Office can answer.

Yours sincerely,

Norman Lynagh, Managing director, Noble Denton Weather Services, London EC1

Phone Service Degradation -- and 911

Scot Wilcoxon <umn-cs!sewilco@datapg.MN.ORG>
23 Oct 87 09:30:00 CDT (Fri)

As reported in RISKS 5.46, on October 17th the sale of World Series tickets in Minneapolis, Minnesota, severely affected telephone service throughout the upper midwest. NW Bell estimates about 200,000 calls were attempted to the sale number in the first hour, and a similar load continued for hours.

Most telephones in the Twin Cities area had delays (with clicking noises) until a dial tone eventually appeared (20-40 seconds on one of my phones and I stopped measuring at 2 minutes on the other). Phone service was slowed throughout the state and in parts of Iowa, Wisconsin, North and South Dakota. Some incoming long-distance callers to other numbers report no problems.

At the customer's request, before the sale Northwestern Bell had set up a temporary choke-type network to restrict the number of calls to the prefix and number from central offices in the area. Despite the restrictions, the sheer volume of calls overwhelmed the network. A NW Bell spokesman says the problem was probably exasperated by customers with automatic redial. Fortunately the sale was not scheduled for a business day.

There were interesting differences between this situation and those caused by broadcast prize giveaways. The first was the large quantity of tickets that stretched the demand over several hours, even after the sellout at 11:30 AM. The Minneapolis-St. Paul toll-free calling area is one of the world's largest, but since every successful caller would get rewarded by being able to buy these prized tickets there were many incoming long-distance call attempts.

Iowa might have had an interesting situation if St. Louis had attempted the same thing at the same time from the south -- a possibility due to the limited time to sell the tickets.

Phone calls for UUCP sites generally failed, since most modems and systems can not detect dial tone. UUCP logs showed 80-85% failure rates during that time. Fortunately, most USENET news transfers in the state are scheduled for times other than the period affected so there was not a large backlog of data trying to flow through most sites.

I will be suggesting to the Minnesota Public Utilities Commission that they try to have 911 protected from this kind of problem. I think the way to reduce giving a delayed dial tone to everyone is to try to give greater delays to people trying to dial a number causing an overload. Preferably also give even greater delays to repeat callers or autodialers. Presently the local

carrier is required to give equal service to everyone, even if that means
giving equally bad service.

Scot E. Wilcoxon sewilco@DataPg.MN.ORG {ems,meccts}!datapg!sewilco
Data Progress Minneapolis, MN, USA +1 612-825-2607

Terrorism

Charles Shub <cdash@boulder.Colorado.EDU>
Thu, 22 Oct 87 22:07:06 MDT

>From: Graeme Hirst <gh%ai.toronto.edu@RELAY.CS.NET> (RISKS-5.47)
>
>In RISKS-5.44, Scott Dorsey (kludge@pyr.gatech.edu) writes: ...
<>Have there been any cases of terrorist or political attacks on comp centers?

Along about 1970 (around the time of Kent State) there was a bombing at the comp center (and a megabuck fire at the student union) at the University of Kansas. I was on my way to the comp center from my office when the bomb went off, and had it not been for some fortuitous circumstances that delayed me that evening, would have been at a terminal about 15 feet from the explosion when it happened. The computer operators suffered some minor injuries and some permanent hearing losses. Our terminal server was a Datanet 30. The explosion blew the doors off it, but it was still running until the machine was shut down. I could probably tell some war stories about the incident, but this digest is not the proper place for that. If anybody is interested, I'll provide more details on the haziness of my recollections privately.

cdash aka cdash@boulder.colorado.edu aka ...hao!boulder!cdash
  aka ...nbires!boulder!cdash aka (303) 593-3492

Terrorism (Re: RISKS-5.45)

WIlliam Swan <uw-beaver!tikal!sigma!bill@RUTGERS.EDU>
Wed, 21 Oct 87 11:10:20 pdt

The computer center at U.C. Santa Barbara was taken over by protesters in the spring of '75. Although the computer room was secured behind locked doors it was easy for them to get control - several demonstrators merely lounged in the hall outside until an operator came, then when she unlocked the door to go in one grabbed her and held the door open for the rest.

One operator inside shut the machine down immediately. Then the protesters ushered (all?) the operators out, and took over the entire building - taping printouts over all the windows and doors. They threatened to destroy the computer if their demands (more money for radical leftist groups) weren't met.

The place was held for several hours (interesting sight: small group of demonstrators just outside the building, group of angry EECS students around *them*) before the police moved in and hauled the demonstrators away. (Another interesting sight: the leaders of the demonstration, very visible throughout

the takeover, managed to vanish just before the police reached the building, leaving the rest to be taken away in the paddy-wagons.)

The machine was not damaged.

Bill Swan sigma!bill

Re: RISKS DIGEST 5.47

Elliott S. Frank <esf00@amdahl.amdahl.com>
23 Oct 87 18:21:36 GMT

In RISKS-5.45, Brent Chapman (koala!brent@lll-tis.arpa) writes:

>Have there been any cases of terrorist or political attacks on comp centers?

During the student riots at Columbia (April, '68), the computer center lobby was briefly 'occupied'. The operators prevented access to the machine room, and the center was then closed and locked for the duration of the disturbance. The occupiers (who included physics grad students and others familiar with the computer center and its operation) were aware that the university's corporate data processing was done on a separate system; that having the administration shut down the computer center was as effective and as disruptive to the routines of the university as shutting it down themselves; and, that due to the pricetags of the equipment involved (several million $$), the administrators might act 'irrationally' to protect the equipment.

Elliott Frank ...!{hplabs,ames,sun}!amdahl!esf00 (408) 746-6384
or ....!{bnrmtv,drivax,hoptoad}!amdahl!esf00

[the above opinions are strictly mine, if anyone's.]

More on password security -- clean up your act

<mccullough.pa@Xerox.COM>
Fri, 23 Oct 87 9:50:09 PDT

from SUN-SPOTS DIGEST Volume 5 : Issue 53

Date: Wed, 14 Oct 87 10:10:38 NOR
From: Jeremy Cook <JMC%NOCMI.bitnet@jade.berkeley.edu>
Subject: Backup procedure

Our systems guy (Tom) came up last Monday evening to backup our Sun. He was new to the job however and didn't know the root password. He phoned Ingolf, but Ingolf didn't know it either so Ingolf, who was meeting Kikki in town, asked Kikki. Kikki phoned in to Tom but the switchboard was closed so the cleaning lady answered. Kikki told the cleaning lady the root password, the cleaning lady went down to Tom and told him and Tom came up to do the backup!

-- Jeremy

Consumer Protection Act

<Richard.S.D'Ippolito@sei.cmu.edu>
Thursday, 22 October 1987 13:24:34 EDT

In RISKS 5.46, there is a discussion by Jonathan Bowen about this Act which states that only a "casual" link is required to be shown between the software product and the injury. I would hope that the correct word is "causal".

Re: UNIX Passwords

<"Russ_Housley.XOSMAR"@Xerox.COM>
23 Oct 87 07:48:57 PDT (Friday)

In RISKS 5.45, Dave Curry explains the process that is used in UNIX to get from a password to an encrypted password. There are other systems that use similar schemes. For example, Multics also uses the low-order seven bits of each character in the ASCII password as input to a cipher routine. Multics uses these bits as both the key and the data.

Dave claims that the truncation of the password to eight characters is not serious. I agree -- if the user knows that only the first eight characters are really being used. When a user enters more that eight characters for the password, UNIX should provide a warning that only the first eight are used. Multics provides such a warning.

Is the "modified DES" used by UNIX a one-way hash?

Russ Housley, Xerox Special Information Systems, Vista Laboratory

Re: UNIX Passwords

Richard Outerbridge <outer%csri.toronto.edu@RELAY.CS.NET>
Thu, 22 Oct 87 00:16:39 EDT

The eight-character limit may have been designed in, but direct mapping into DES keys is no feature. The average entropy of English is about one bit per letter over blocks of eight or more letters; so rather than 56 bits of equivocation the routine assuredly provides eight. Hashing long strings together using CBC or CFB message authentication techniques yields eight byte hex strings in which every last trace of equivocation is present in a 'random' looking pattern. Time for a change of password routines.

Use of Social Security Numbers

James Peterson <peterson@MCC.COM>
Thu, 22 Oct 87 21:41:35 CDT

We know that the new tax law requires a Social Security number for each dependent age 5 or older (if you want to list them as a deduction). Our school district is doing its part to make this easier for parents (and themselves). They are required "to identify students with either a Social Security number or an assigned number." Since many kids may not have an SS number, they have sent home a form to fill out to apply for a number. The school will provide copies of their (the school's) records to SS as part of the application for SS, and the SS cards will be distributed through the school.

Of course, the form (that HAS to be returned) includes six options including (1) My child already has a social security number of ___ __ ____ (2) We have already applied; I will notify the school of the number when it arrives, (3) ...

There is no option for (7) My child has one and it is not to be used to identify school records.

Search RISKS using swish-e

Report problems with the web pages to the maintainer

Search RISKS using swish-e

THE RISKS DIGEST

Forum on Risks to the Public in Computers and Related Systems

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

Volume 5: Issue 49

Monday, 26 October 1987

Contents

Freak winds in southern England

<sufrin%prg.oxford.ac.uk@NSS.Cs.Ucl.AC.UK>
Sat Oct 24 23:56:06 1987

I wonder what the average English resident would have done if there HAD been advanced warning of last week's hurricane? My guess is that the most probable reactions would have been something like:

1. Don't be silly; this is England.

2. Let's take the kids outside and watch.

The Oxford Literati would of course have rushed around quoting

Bernard Shaw (Pygmalion) to the effect that

"In Hereford, Hertford and Hampshire, hurricanes hardly happen".

"I must go and tie the roof of my house down, and make sure that my neighbours' chimneys and trees are all secure" comes in way at the bottom of my list of likely reactions, and I can't help asking what the emergency services or the utility companies COULD have done if they had known a few hours earlier (apart from cancelling leave).

Perhaps the weather forecasters did us all a favour! There would have been many more casualties if there had been a lot of people outside watching. There may even have been more casualties from panic if the forecasters had known and had made clear what to expect, and where to expect it. Certainly neither the military nor the civilian emergency forces here are prepared for mass evacuations of the kind that might have saved some of the lives that were lost. (They usually claim to be astonished when it snows more than a couple of inches in an evening).

Do I hear you ask "what's this got to do with the risks of using computers?" I worked very late at the computing Lab on the eve of the Hurricane, tumbled into bed at about 2:30am, and slept through the whole thing.

Freak winds in southern England

Franklin Anthes <mcvax!geocub!anthes@uunet.UU.NET>
Fri, 23 Oct 87 14:50:12 +0200

Maybe it was unexpected in the UK, but here in France there were storm warnings on the midday news. They said that a very strong storm was forecast, and sure enough that night some parts of France had 220km/h winds.

I know that "la meteorologie nationale" here in France has a Cray for their forecasting. Maybe the UK doesn't have such high-powered computers? Or maybe French weather forecasters are just better:-):-)

Frank Anthes-Harper
Usenet: ....!ucbvax!decvax!uunet!mcvax!inria!geocub!anthes

On the Risks of Using Words That Sound Similar

Bruce N. Baker <BNBaker@KL.SRI.Com>
Mon 26 Oct 87 09:41:59-PST

In RISKS 5.48, Richard S.D. D'Ippolito points out the substitution of the word "casual" where "causal" was intended. The difference is significant. I see more and more of this type of problem as we become dependent on spelling checkers that accept properly spelled words even though they completely distort the meaning. Words that sound similar and look similar to a secretary are especially a problem.

In the same issue, Scot E. Wilcoxon's contribution regarding Phone Service Degradation and 911 uses the word "exasperated" when "exacerbated" was intended. The meaning still comes through, and in a few years, if enough secretaries type the one word when it should have been the other, the two will appear as synonyms, similar to the way "scan" and "skim" have evolved. "Apprise" and "appraise", and "foundering" and "floundering" will soon suffer the same fate. No one seems to understand "affect" vs. "effect" anymore so we might as well list them as alternative spellings of the same word. It might be a bit more dangerous when we equate "enervating" and "invigorating". Not even Webster seems to care about preserving the distinction between "aggravate" and "irritate". Of course, Webster merely reflects the bad usage we impose on our language, and often secretaries merely mirror the bad usage of the writing they receive. So now "terrific" lists just about any context you may wish to give the word. But surprisingly, "livid" does not equate with "angry" in my 1971 version of Webster. Surely, that has been "corrected" by now. "Erstwhile" still does not have "distinguished" as one of its meanings so maybe there is some hope.

I guess my point of all of this is that some of us still care about the original intent of words. No, this will not make the transition to the original intent of the framers of the Constitution. As a former professor, I was astounded at how many students were upset by my corrections to their grammar. Often, I heard, "I didn't know we were supposed to proofread our papers," or "I didn't realize this was an English class, I thought it was a course in the business school."

How vulnerable I am. I am sure there must be at least 10 errors in word usage and "grammer" here, but that won't "effect" me at all.

[I try to fix obvious screwups when possible. There are times (such as today) when I have a very limited window on-line (and 40 backlogged messages -- too many of them on UNIX passwords). This afternoon I had a net connection that would give me only a few echoed characters, sometimes with more than five-minute delays. PLEASE try to edit your own messages more carefully, and don't be surprised when your incoherent contributions are not included. Also, I'm getting a lot of UNIX password stuff that heavily duplicates earlier messages. I can guess that some of you are still getting mail many days late... or just don't like to read. PGN]

CD, Terrorism, Stocks (Previous 3 RISKS)

<JPAnderson@DOCKMASTER.ARPA>
Fri, 23 Oct 87 15:08 EDT

The last 3 RISKS prompted some responses.

Re: "Civil Disobedience"

From what I have seen this kind of behavior is not very CIVIL! It is also an example of the debasement of the language (language in the pits) practiced by certain newspapers and even radio and TV stations --

euphemisms to replace (and distort) reality. "Civil Disobedience" is actually at the minimum a misdemeanor called Disturbing the Peace. Unders some circumstances, I would agree with the writer who claimed it was terrorism. Certainly mobs, no matter how well intentioned are not engaged in CIVIL behavior. Often, these little excursions boder on riots. Of course, they are not called any of these things, particularly since newspapers, radios and TV started calling strikes (often illegal, and unauthorized) 'Job Actions'. When I was growing up, most of the 'Job Actions' of Teachers, Civil Servants of various kinds and other employee groups (like the NFL players) were called strikes, or sometimes WILDCAT strikes (meaning they were illegal and/or unsanctioned by the parent organization). So, spare me the "Civil Disobedience", "Job Actions", and while we are at it, "Methodology".

Re: Stocks into Bondage

It is interesting, considering the volume and panic, that the NYSE computer systems did NOT fail, even though they were sure overloaded, and continued to be a couple of hours late in reporting trades. An 'atta boy" to the designers and implementers of those systems.

Cheers, Jim

The Stock Market Computers and SDI

Bob Berger <berger@datacube.com>
Sun, 25 Oct 87 20:28:48 EST

I hope that the experience of a large network of computers doing something unplanned for such as accelerating the crash of the stock market will make the "Decision Makers" stand up and take notice!

The network of computers that makes up the stock trading system is much less complicated than what the SDI planners are calling for, yet the stock computers behaved in unexpected ways that were bad for most people involved. In this case it was only that some people lost millions and a major fracture had been put in the stability of Western Society's economic structure.....
Bob Berger

Datacube Inc. Systems / Software Group 4 Dearborn Rd. Peabody, Ma 01960
VOICE: 617-535-6644; FAX: (617) 535-5643; TWX: (710) 347-0125
UUCP: berger@datacube.COM, rutgers!datacube!berger, ihnp4!datacube!berger
{cbosgd,cuae2,mit-eddie}!mirror!datacube!berger

[Remember, Jim is talking about the transaction processing and Bob is talking about programmed trading feedback instabilities... PGN]

(Almost too much of) Password Encryption

Matt Bishop <bishop%bear.dartmouth.edu@RELAY.CS.NET>

Sun, 25 Oct 87 10:30:28 EST

A little comment on UNIX password encryption. It may be very redundent.
[Yes, it is, but perhaps if people will read it, they will stop submitting suboptimal communications. PGN]

In RISKS 5.48, "Russ_Housley.XOSMAR"@Xerox.COM asks if the "modified DES" is a one-way hash. Nope. The modified DES just encrypts the null message (all 0's) with the password as key and maps the result to a 64-character alphabet. That, plus a code indicating which modification is used, is stored on line. When a user logs in the password he supplies is used to repeat this procedure, and the result of that is compared to the (stored) value. If they agree, the password is right and the user is logged in. If not, the password is not correct and the user is not logged in.

The modification, incidentally, is to perturb the E table in one of 4096 ways and apply that DES 25 times in succession. (That is, the output of the first is the message for the second, the key being the password in all iterations.) The idea is that the perturbation prevents dictionary searches for a large number of passwords by forcing the password algorithm to be run once for each possible password AND for each already-encrypted password (that is, instead of just encrypting a 25,000 word dictionary and comparing the result against each of 100 encrypted passwords, an attacker has to encrypt the 25,000 word dictionary once for each encrypted password; this is equivalent to 2,500,000 encryptions.) Hence, the time for such a search should be unacceptably high.

Matt Bishop

bishop%bear.dartmouth.edu@relay.cs.net
...!decvax!dartvax!bear!bishop

UNIX Passwords

Mark Brader <msb@sq.com>
Fri, 23 Oct 87 22:49:32 EDT

> The truncation of UNIX passwords to 8 characters is not a bug, it's a
> feature. If you have source, examine the code to libc/gen/crypt.c.
> Your password is *not* actually encrypted on UNIX. Rather, it is used
> as the *key* to encrypt a standard block of text ...

and since DES has 56-bit keys, the password has to be reduced to 8 7-bit characters. True, but taking the *first 8* characters is about the worst method I can think of for reducing a long password to 56 bits! I've never been satisfied with this aspect of UNIX; I want 12 significant characters in my passwords (and all alphabetic, please, so I can type them *fast*).

Taking the *last* 8 characters would be a distinct improvement, because it's necessary to pause a moment before entering the password, and people tend to use that moment to reach for the first key or two of the password.

Better yet would be to use a simple hashing function to map the long password onto the 56-bit space. Even something as simple as XORing the 1st, 9th, 17th, etc. characters into the first 7 bits, and likewise for the other positions, will ensure that any small change to any part of the password generates an incorrect password. With a space of 72,057,594,037,927,936 hash buckets, it makes no practical difference that there are now many alternate passwords that yield the same 56-bit sequence.

(The same technique would also be useful for any banks that come to their senses and allow 12-digit PINs for ATM use -- around here they're all either 4 or 6 as far as I know, and mostly without privacy shields on the keypads -- but which think it's much too much work to change their file format.)

It also wouldn't hurt to "personalize" and keep secret the "standard block of text" that is encrypted using the 56-bit key; this would inhibit some kinds of password searching done on a different UNIX machine by someone who gets a copy of the password file (with the "encrypted passwords"). This is best done when the machine is acquired, as it invalidates all existing passwords.

Any of the steps described above would make it impossible to simply copy a password file onto, or from, an unmodified UNIX system and use it. Whether this is an advantage or disadvantage depends on the situation.

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

> If ... it seems easier to subvert UNIX systems than most other systems, the impression is a false one. The subversion techniques are the same. It is just that it is often easier to write, install, and use programs on UNIX systems than on most other systems, and that is why the UNIX system was designed in the first place.
>
> -- Frederick T. Grampp & Robert H. Morris

Re: Phone Service Degradation -- and 911

Rich <RMRichardson.PA@Xerox.COM>
25 Oct 87 21:48:09 PST (Sunday)

From: umn-cs!sewilco@datapg.MN.ORG (Scot Wilcoxon)
> I will be suggesting to the Minnesota Public Utilities Commission
> that they try to have 911 protected from this kind of problem. I
> think the way to reduce giving a delayed dial tone to everyone is
> to try to give greater delays to people trying to dial a number
> causing an overload. Preferably also give even greater delays to
> repeat callers or autodialers. Presently the local carrier is
> required to give equal service to everyone, even if that means
> giving equally bad service.

Pardon me, but there seems to be an assumption in here that just isn't true. When you say "... give greater delays to people trying to dial a number causing an overload," you are assuming the telephone exchange knows which number is to be called before it gives a dial tone to the caller. But you

see, the dial tone is given so the caller may send the number to be called to the exchange. If the exchange can predict the number to be called, dial tones are unnecessary (along with half the equipment in your phone!).

Rich

[Hmm... I interpreted the suggestion as delaying the NEXT dial tone. PGN]

INUSE.COM Program

Chris McDonald STEWS-SD 678-2814 <cmcdonal@wsmr05.ARPA>
Mon, 26 Oct 87 7:56:32 MST

As a matter of policy we require automatic timeout features on our systems, where feasible, to disconnect inactive terminals. The thinking is that in most cases an "inactive" terminal in our environment denotes that a user has left his or her device unattended. Hopefully the timeout program may save a user from his or her own carelessness and preclude another person from "masquerading".

You might expect that not all users are that enthusiastic about the program. On some of our VMS hosts several personnel use a DCL command file generally named INUSE.COM. The program formats the screen to show "Terminal in Use" in theory one must know the password to then gain access to the terminal. At least that was what many users thought!

When we finally began to install the Version 4 update of VMS, we found that DEC had implemented a recall function. By entering a Ctrl Y and pressing the up arrow on the terminal a user could recall the last input to the screen. So logically, if the last input was the password, then . . .?

We found it rather ironic that users thought they had protected themselves and defeated our automatic timeout program at the same time. The INUSE.COM program can be modified to address the recall function.

Free phone-calls

<SBQBEB%HLERUL57.BITNET@wiscvm.wisc.edu>
Mon, 26 Oct 87 14:35 N

E.van Batenburg, Instituut v.Theoretische Biologie, Groenhovenstraat 5
2321BT Leiden Holland (tel.071-132298)

The Dutch "Personal Computer Magazine" revealed in its september issue how hackers in Holland managed to fool the telephone company and got free phone-calls to everywhere in the world.
First they ring 06 which announces to the Dutch telephone computer that a "collect" call is to be dialed.
Next they choose a number in Denmark (which one was unfortunately/fortunately, depending on your point of view, not revealed) which let the Danish computer reply to Holland that the call is accepted.

Finally they dial their proper destination.

The Dutch telephone company reacted rather grumpy to this disclosure.
They stated that PCM is stimulating abuse of the telephone.
According to them they have no means to correct this on short notice
because the Danish computer is at fault and they are waiting for a
complete overhaul of the Danish telephone computer.

It is not clear who (if anybody) is paying the costs for those calls.
Eke van Batenburg

Search RISKS using swish-e

Report problems with the web pages to the maintainer

Search RISKS using swish-e

THE RISKS DIGEST

Forum on Risks to the Public in Computers and Related Systems

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

Volume 5: Issue 50

Tuesday, 27 October 1987

Contents

Weather (Re: RISKS 5.45)

<willis@rand-unix.ARPA>
Tue, 27 Oct 87 10:46:00 PST

Here's a contribution to the big blow in England. I was scheduled to land at Heathrow the morning of the 16th and we sat at Dublin for 6 hours waiting for the storm to clear. The weather at Dublin was clear and calm.

My comments are based on my participating in an NRC study for NOAA a few years back; it concerned future needs for computer support to weather models. I'm giving you this from memory but I'm sure that the general facts are correct.

Within the last 10-15 years or so, there were two examples of severe weather in this country that forecasters missed: the Johntown flood in western Pennsylvania from unprecedented rains, and the big blizzard in the Northeast, which interestingly had been forecast by a smallish private weather service used by some of the trucking companies. The explanation from the weather types was that each of them had been a mesoscale

phenomenon -- too small to be included or visible in the global weather models but too large to fall within the capabilities of local forecasters.

The mesoscale effects seemingly had been overlooked by the WX types and had just been appreciated at the time we were doing our study.

The large 5-day weather models which typically run once or twice each day on some huge computer are upper atmosphere models. They work at a prescribed pressure profile which it seems to me is 200 millibars, corresponding roughly to jet altitudes. As such they predict the large effects in weather patterns.

The local forecaster uses inputs from satellites, from the large models, and from local and nearby data sources. But his ability to predict is limited to an area perhaps 100 miles or so across.

The mesoscale phenomena are a few-to-several hundred miles in extent and are lower atmosphere behavior. The WX types have two problems in getting models to handle them: first, building the models themselves which must include things that the upper atmosphere models can ignore (e.g., topographic effects, ground-air heat transfer, effects of large lakes and/or rivers), and getting the data to drive the models. The models will have to have a very fine mesh to handle the detail needed, and consequently the data sources will also have to be fine grained.

As of 7-10 years ago, the work on the models was just starting. I do not know the present status.

I suspect that the London and southern England storm was mesoscale in size. It definitely was neither a tornado nor a hurricane although both labels were used by the media. It clobbered an area a few hundred miles across but Ireland was untouched. In addition since the English weather often comes from the west, there is a lack of weather observations to drive any models or forecasts. Aircraft are too high for the observations needed by mesoscale models, and surface vessels do not normally send up WX balloons nor take the usual WX measurements.

The damage to London and southern England was stupendous. Some of the parks (e.g., Hyde Park) were closed because of the amount of downed trees, broken branches and trash. Flooding was extensive and one train ran into a river when the undermined bridge gave way. Winds in London were the highest ever recorded. The problems continued through the following week. Reporting on the telly was confined primarily to damage; there were only a few comments about the failure to forecast but no recriminations or blaming. No mention of mesoscale effects either.

Relevance of all this to RISKS: you never can be sure how well a model represents the real world that it purports to describe and mimic.

Weather Prediction in UK

"ZZASSGL" <ZZASSGL@CMS.UMRCC.AC.UK>

Tue, 27 Oct 87 11:29:35 GMT

1. The UK met office uses a Cyber 205 to prepare its forecasts - It also predicted bad weather over north France. The problem was that the weather had not read the forecast and moved north very rapidly after the last forecast run of the day.
2. Without exception the British press has blamed the "computer" for the lack of warning of bad weather. Now we all know that unless there was some sort of hardware problem(which there wasn't) it is the software that may, and only may, be at fault. Is this confusion a "risk"? It is certainly a misconception and if future funding of the UK Met office is cut as a result is will surely be a risk to all the people who depend on the very good work that is done there.

Geoff. Lane.
University of Manchester Regional Computer Centre

Weather and terrorism (separate)

<eugene@ames-nas.arpa>
27 Oct 87 11:12:48 PST (Tue)

> Cyber 205 supercomputer as part of its investigation following last week's
> hurricane-force winds. The office has been criticised for failing to
> predict the speed and path of the storm...
>
>My understanding is the main reasons for lack of success in predicting
>the winds were a) lack of data (the storm came from over the sea --
>fairly normal in Britain! -- where there are few weather stations) and
>b) lack of computing power (and lack of good algorithms?).

Please don't completely equate computing power to the problem of these models. Also don't blame machine manufacturer (we have both a 205 and an X-MP/48). There was a recent Scientific American article on the problems of weather models (cover was a grid), but a better article appears:

%A Joseph J. Tribbia
%A Richard A. Anthes
%Z NCAR
%T Scientific Basis of Modern Weather Prediction
%J Science
%V 237
%N 4814
%D 31 July 1987
%P 493-499

There is a specific section on why forecasts are inaccurate. It's not just algorithms. The equations of weather are basically good equations. Read the article, its more detailed than I wish to summarize here.

>Subject: Terrorism (Re: RISKS-5.45)
>

>The computer center at U.C. Santa Barbara was taken over by protesters in
>the spring of '75. Although the computer room was secured behind locked
>. . .
>One operator inside shut the machine down immediately. Then the protesters
>ushered (all?) the operators out, and took over the entire building - taping
>printouts over all the windows and doors. They threatened to destroy the
>computer if their demands (more money for radical leftist groups) weren't met.
>
>Bill Swan sigma!bill

Hi Bill--
Yes, Don Davis told us about when he was kicked out. I did not recall
it was for "radical leftist groups," unless you count the Chicano Studies
program as such. We have to be careful in distinguishing political judgments.
(Are computer people naturally conservative?)

My suggestion is that if the original requester is interested
in acts of terrorism against computers, contact Computerworld
or maybe Donn Parker (SRI) might have a list. CW did publish
a list of acts including the bombing (and death) at Wisconsin in
the 1970s, and several bombings in Europe. Happens ALL the time.

--eugene miya

Civil disobedience

David Redell <redell@src.dec.com>
Tue, 27 Oct 87 11:18:05 PST

Re: Jim Anderson's complaints about the term "Civil Disobedience"

One may admire or despise some or all acts or practitioners of civil
disobedience, but it's simply incorrect to claim that the term stems
from efforts of contemporary newspapers, radio and TV to distort reality
with euphemisms implying polite behavior. The term originated in the
mid-19th Century and has nothing to do with "civil" as in "civility".
It is based on "civil" as in "civil rights" or "civil servant" -- that is

> civil (adj) 1 a: of or relating to citizens; b: of or relating to
> the state or its citizenry;... 5: of, relating to, or involving
> the general public...

Dave Redell

Reported Japanese Autopilot Problems

Nancy Leveson <nancy%murphy.uci.edu@ROME.UCI.EDU>
Tue, 27 Oct 87 19:53:14 -0800

Last week somebody told me that Dan Rather had reported that a Japanese
plane, the MU-2, has had 100 crashes which have now been traced to a

computer problem. Supposedly, the computerized autopilot will, under certain conditions, not let the pilot have control back. I did not hear this myself and since nobody has reported it in Risks, I have a suspicion that the story is not correct. Did anyone hear the Dan Rather telecast?

Nancy

Amusing bug: Business Week Computer (F)ails

GW Ryan <gwr@garage.nj.att.com>
24 Oct 87 13:03:31 EDT (Sat)

The following paragraph is taken (without permission) from p. 14 of the November 2 "Business Week". I thought it was an amusing little bug report. I tried to imagine how it could happen... you'd think we'd have alphabetical order down pat by now!

> Some copies of our special bonus issue,
> The Corporate Elite: Chief Executives of
> the Business Week Top 1000, contain
> mistakes in the alphabetical index of
> chief executives on pages 341-350 and in
> the guide to how to read the CEO profiles
> on page 350. Because of a computer problem,
> certain letter combinations with "f" were
> omitted from company names and the guide.

jerry ryan (allegra!cord!gwr) Bell Labs, Liberty Corner NJ

Television series "Welcome to my world"

Clive Feather <mcvax!root.co.uk!cdwf@uunet.UU.NET>
27 Oct 87 13:25:43 GMT

There is a new series on BBC1 television called "Welcome to my World" which raises some of the topics we are / ought to be discussing. Anyone out there seen it and got any comments ?

It's on BBC1, Sundays, at 2305 until 2335.

Clive D.W. Feather +44 1 606 7799 x 235

Search RISKS using swish-e

THE RISKS DIGEST

Forum on Risks to the Public in Computers and Related Systems

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

Volume 5: Issue 51

Wednesday, 28 October 1987

Contents

Re: Reported Japanese Autopilot Problems

Will Martin -- AMXAL-RI <wmartin@ALMSA-1.ARPA>
Wed, 28 Oct 87 10:56:58 CST

Yes, I heard that report, and watched most of it (I was in the kitchen at the time and it was on the tiny-screen set on top of the fridge, and I was doing other things at the same time, but I caught the gist).

The particular plane is a corporate turboprop, and there have been repeated instances of crashes at high speed into the ground. Recordings of pilot-to-tower conversations indicate that the autopilot has had a history of seizing control away from the human pilot, and that turning it off again is sometimes difficult or impossible. (There weren't many details; I am guessing that to disable it the pilot has to hit circuit breakers or otherwise power down the autopilot, and it may be hard to do when he is also wrestling with the controls to try to keep the plane from crashing.) Could it be that, this being a corporate plane, there is

normally only a single pilot, not a pair (pilot & copilot), so there are no free hands to fiddle about with such switches or seldom-used controls? (That's just an unsupported speculation on my part...)

In any case, it was a for-real broadcast. You might be able to get a transcript from CBS or from one of the video-news-recording/clipping services. (Side note to the list: Does anyone have a comprehensive list of such video-clipping services? I've heard of them several times, and it seems that people often need to get such info, like in this case, after hearing about a televised report or event that they missed. I don't know any specific firm or organization names or locations, nor have I any idea of what such services cost.)

Regards, Will Martin

(Non-)Japanese Autopilot Problems

Joe Morris (jcmorris@mitre.arpa) <jcmorris@mitre.arpa>
Wed, 28 Oct 87 12:43:39 EST

In RISKS 5:50, Nancy Leveson writes:

> Supposedly, the [Japanese MU-2's] computerized autopilot will, under
> certain conditions, not let the pilot have control back.

I think you'll find that most autopilots -- indeed, most avionics of any type -- in American-registered aircraft will be American-manufactured. At least at the low and middle end (I can't speak for the high-priced spread types) there isn't much penetration by foreign manufacturers. While I've never flown the MU-2, my memory says that those I've seen had either King, Bendix, or Sperry avionics packages, probably with a matching IFCS (Integrated Flight Control System).

I recall seeing some MU-2 accident reports a while back that referred to the autopilot as being involved, including one in which the pilot told the FAA controller that he had autopilot problems just before the (fatal) crash. I'm inclined to doubt that "the autopilot would not let the pilot have control back", since the control servo drives the (mechanical) control wire through a slip clutch whose breakaway limit must be no greater than can be overcome by the pilot. It would require a runaway autopilot *and* a siezed clutch to deny the pilot control.

The MU-2 has a reputation of requiring an unusually high degree of attention by the pilot, so any autopilot problems could be more serious in a MU-2 than the same problem would be in, say, a Cessna 421.

What may be more likely is that the autopilot sets up divergent oscillation which ultimately overstresses the airframe. If for some reason the pilot fails to disconnect the autopilot promptly, the result can be spacial disorientation which in turn can cause the pilot to lose control of the aircraft even if the autopilot-induced load was within limits.

What does this mean to RISKS-readers? One problem which is found in many aviation accident reports is that the aircrew (student pilot through 747 captain) has become complacent due to the assistance given by the "black boxes" on the aircraft. When one of those boxes fails, the sudden transition to basic flying and navigation (probably not practiced for a l-o-n-g time) isn't successful and the airplane does things it's not supposed to. Even worse, the boxes can give false or conflicting data and the aircrew doesn't resolve the problem in time to prevent an accident, like a 727 did a few years ago in New York when its stall warning (in effect, underspeed...no flames, please) and Mach warning (overspeed) alarms both activated. The result was a "superstall" and crash with no survivers...straight down from 30,000 feet.

Possible nuclear launch prevented by parked vehicle

Scot Wilcoxon <umn-cs!sewilco@datapg.MN.ORG>
28 Oct 87 12:23:56 CST (Wed)

Nearly three years ago a malfunctioning guidance system caused indication of a launch sequence on a Minuteman 3 missile with three nuclear warheads. An armored vehicle was then parked on the silo to block any accidental launch.

AP reported that a Wednesday story in the Casper Star Tribune says the guidance system malfunctioned on January 10, 1984. Capt. Bill Kalton of Warren Air Force base says that lights which monitor the status of the missile followed the pattern of a launch. When the guidance system failed it showed false indications on the monitoring equipment.

A response team rushed to the missile site, parked an armored vehicle on top of the silo and left the scene. If the concrete cover of the silo had opened the vehicle would have fallen on the missile, damaging it and blocking its path. A maintenance team determined the missile was not in a launch sequence and that the warheads were not armed.

Scot E. Wilcoxon sewilco@DataPg.MN.ORG {ems,meccts}!datapg!sewilco
Data Progress Minneapolis, MN, USA +1 612-825-2607

SDI information system announced

Scot Wilcoxon <umn-cs!sewilco@datapg.MN.ORG>
28 Oct 87 12:23:33 CST (Wed)

AP reports that the Pentagon has created a computer-based system to encourage communication of SDI technology. Col. Jim Ball, director of technology applications for the SDI Organization, made the announcement. Using TAIS, "a civilian researcher working on a field also being explored for Star Wars can obtain an unclassified summary of the Star Wars work and a referral to the individual researcher for consultation."

The TAIS computer will not have classified information and will be available at only the cost of a phone call. U.S. citizens, after

agreeing not to disclose sensitive information, can apply to the Defense Logistics agency for an access code. No security clearance is needed, although the Pentagon considers some information as being sensitive enough to keep track of those who have access.

Scot E. Wilcoxon sewilco@DataPg.MN.ORG {ems,meccts}!datapg!sewilco
Data Progress Minneapolis, MN, USA +1 612-825-2607

'Computers In Battle'

Rodney Hoffman <Hoffman.es@Xerox.COM>
28 Oct 87 07:25:03 PST (Wednesday)

A brand new book of interest:

'Computers In Battle' edited by David Bellin and Gary Chapman.
Harcourt Brace Jovanovich, 1987, $14.95.
xiv + 362 pages, including Bibliography, Resources, Index.
ISBN 0-15-121232-5

Table of Contents

Computers and War: Philosophical Reflections on Ends and Means
John Ladd

Amusing bug: Business Week Computer (F)ails

John Pershing <PERSHNG@ibm.com>
28 October 1987, 09:44:47 EST

Just an educated guess, but the failure was probably due to the index generation software not recognizing ligatures (e.g., 'fl' and 'ffl'), which were stored as single, "non-alphabetic" characters.

John A. Pershing Jr., Yorktown Heights

[Ligature software carefully before using it. PGN]

Civil Disobedience

Fred Baube <fbaube@note.nsf.gov>
Wed, 28 Oct 87 10:38:58 -0500

An important element of civil disobedience is that you take your lumps as they are determined by the system whose legitimacy you are challenging. Thus the blacks who sat in the front of the buses and accepted arrest were practicing civil disobedience, in the hope that the visibility would create the public sentiment for change.

In a republic such as ours, CD provides an important avenue of political expression, when the "approved" methods (writing legislators, organizing, bumperstickers) don't cut the mustard.

[OK... I think we have saturated on this one for now. TNX... PGN.]

Search RISKS using swish-e

THE RISKS DIGEST

Forum on Risks to the Public in Computers and Related Systems

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

Volume 5: Issue 52

Saturday, 31 October 1987

Contents

Risks in intelligent security algorithms

Peter J. Denning <pjd@riacs.edu>
Fri, 30 Oct 87 13:25:45 pst

On October 29 I was ensnared by a design flaw in the security system of the parking garage of the San Francisco airport. The same system is undoubtedly used at other airports. I had returned from a trip that morning and paid $88 for 8 days. I returned the same evening to fetch my wife, who returned from a trip. On presenting my ticket, the attendant said the computer said I owed $99, rather than the $1 I was expecting to pay. Guards appeared and instructed us to go to the garage office to discuss the matter with garage

officials. After some discussion the garage official allowed us to leave, paying $1.

Here's what happened. The garage security system is set up to prevent a customer from obtaining a second entry ticket on his return and thereby underpaying. When I entered the garage 8 days ago, a video camera recorded my license number and associated it the parking ticket dispensed by the machine; the resulting license-ticket entry record was placed in a database later that night. When I checked out, an exit record of my license-ticket pair was made, and scheduled to cancel the entry record during the late night computer run. However, when I attempted to check out the second time, I had not been there long enough for a new license-ticket entry record to be placed in the database; accordingly the standard database check found the still unpurged record of my first entry and computed that I owed for 9 days.

The garage official apologized for the inconvenience and said the system is needed to prevent fraud and occasionally someone stumbles into a false alarm. There is no interest in changing the system or posting notices warning customers to keep their receipts if they return to the garage a second time in one day.

Computer's Normal Operation Delays Royal Visit

Mark Brader <msb@sq.com>
Thu, 29 Oct 87 14:18:17 EST

From an article in MODERN RAILWAYS, September 1987, by Roger Ford, on the opening of the Docklands Light Railway (DLR) in London. Submitted to RISKS (and slightly edited) by Mark Brader:

Ironically, the 'problems' the daily press reported at the Royal Opening were caused by the automatic system working properly. The royal train (number E2R -- a nice touch that) was timetabled to leave Island Gardens station at 15:30. As the royal party was early, the control room dispatched the train manually rather than keep Her Majesty waiting for five minutes.

This meant overriding the computer, which was operating in regulated mode. Unfortunately, computers are less sensitive to royal protocol, and when E2R arrived at Mud Chute station [!] five minutes early, it was given a "dwell time" of several minutes to bring it in line with the timetable.

If you happen to be on board a stationary train with your Sovereign, two minutes is a very long time, so the train captain reverted to manual ...

One of the golden rules for bodyguards is that you leave a vehicle or building first. As the train rolled to a halt in Poplar station, a security man used the emergency exit so he could get out first. Not only did this stop the train by interrupting the door-safety interlock circuit, it stopped it short of the docking beacon. Unless the train receives a message from the beacon it does not know it is in a station and the doors won't open.

I was standing next to the manager of the doorgear suppliers at the time and can vouch for the fact that time also stretches agonisingly when there is the possibility that Her Majesty is being isolated from her loyal subjects in Docklands by your product!

In the light of this, I wonder whether anyone has thought to give the police and counter-terrorist organisations a briefing on the features of automatic railway operation.

Public notice of a security leak

<RCOPROB%HDETUD1.BITNET@wiscvm.wisc.edu>
Wed, 28 Oct 87 21:18:02 MET

From: Rob van Hoboken +31 15 78-3813 RCOPROB at HDETUD1

I found the following gem in issue 10 (July 1987) of MVS update, a publication of Xephon aimed at the MVS systems programmer.

> Dynamically making programs APF authorized
>
> The following procedure should work under any release of MVS.
>
> The standard way of making progrmas APF authorised is to link them into an
> authorised library specified in the SYS1.PARMLIB member IEAAPFnn with the
> link-edit attibute of AC=1. Changes to such a library specification will
> require a re-IPL.
> If authorised programs are to be executed under TSO, they must be put into
> a table in the Link Pack Area: TSO commands go into table IKJEFTE2 and called
> programs go into IKJEFTE8. Any changes to these tables require a re-IPL
> with the CLP option to make them effective.
> It is, therefore, convenient to be able to turn on and off the APF
> authorisation dynamically for any program that does not have the AC=1
> attribute, in any library upon request.
> Just be aware that this can be a security exposure.
> The solution:
> The method is to have a user SVC that sets or removes the APF bit in the
> control block JSCB. This SVC is probably well known but it is, together
> with the following two macros, a pre-requisite to many homegrown functions
> that help to make life easier.
> The following SVC can be enhanced by adding installation dependent security
> checks:
> * authorisation svc 235 type 4
> * r0 = 1 turns on auth
> * r0 ne 1 turns off auth
> *
> code follows

Personally I would rather omit the name of the author to protect the guilty (but most of all his company), but since there was a copyright statement on the publication:
(C) Nils Plum, Systems Programmer (Denmark).

In effect this persons describes a hole in his installation, and proudly tells us that many of his tools depend on it. Probably (I've seen it in several installations) the "installation dependent security checks" were removed at some time to make "all those goodies available to us users".

The worst part is that a lot of software companies ship out programs that actually need these kind of trapdoors to function at all. I have written to some of these companies with a description of the problem, proof of its existence and a work around. I got laughed at, made rediculous and told to not to spread the word. One of these people (a real big company!!!) even told me: (direct quote!)
"it must be safe, even the CIA uses it"

Can anyone help me to a userid + phone number on either Mr. Plum's installation or the CIA?

Rob van Hoboken, Delft University of Technology, Computing Center

---

sc.4.1 update dangerous

Fen Labalme <sun!megatest!elvis.fen@ucbvax.Berkeley.EDU>
29 Oct 87 12:25:42 PST (Thu)

The new release (4.1) to the public domain spreadsheet "sc" has a noncompatible change that, along with an overlapping windows Sun environment and an ambiguous (but fairly standard) naming convention, conspired to destroy a database.

I maintain a database of members of a Spring Water Cooperative at my workplace in North San Jose. Each member contributes $3 a month to enjoy unlimited use of a bottled water cooler. The record of accounts is kept in a database maintained by sc.

The entry for a member for any particular month (say, [K1]) is the minimum of the total_amount_contributed [A7] minus the sum of payments so far [@sum(d7:J7)] and the current ammount due [K0]. As a sc.3.1 expression, [@min(A7-@sum(D7:J7),K0)].

This morning our /usr/local manager installed sc.4.1 naming it /usr/local/bin/sc (simply replacing its predecessor).

Soon after, a member gave me his dues for the month. I opened sc in a window that had its right half hidden by an overlapping window, yet I had access to the total_amount_contributed column. Thus I did not notice that the right half of the spreadsheet was blank! I updated his account and saved the database.

What I didn't realize is that sc.4.1 didn't recognize this usage of @min(), as this had changed, and when it saved the database, it simply and quietly ignored (read: deleted) all of the entries which it didn't "understand".

Thank Zippy for disk-to-paper dumps!
-fen

P.S. I am sorry to see this useful function disappear. The README states that the "range" function should be used in its stead, but I havn't yet figured out how. Old and new expressions for table entries appear below:

old: @min(A7-@sum(D7:J7),K0)
new: A7-@sum(D7:J7)<K0?A7-@sum(D7:J7):K0

Fen Labalme, Megatest Corp, VLSI Systems Division, 880 Fox Lane, San Jose, CA 95131 (408) 437-9700 x3382
"megatest!fen"@riacs.ARPA UUCP: ucbvax!sun!megatest!fen

Mitsubishi MU-2 problems

Peter Ladkin <ladkin@kestrel.ARPA>
Fri, 30 Oct 87 11:07:59 PDT

if anyone would like detailed knowledge of the mu-2 accident rate, i can look up some analyses i have. please send me mail.

roughly, there have been a number of unexplained `uncontrolled descents into terrain' with the mu-2. of the order of a dozen, mostly with experienced pilots, although not with a lot of mu-2 experience. some others that have been explained concern the proper operation of the autopilot. autopilots with altitude hold can enter an unstable feedback loop. e.g. the plane is trimmed to hold altitude, and deviates, say down. the pilot pulls up, whereupon the autopilot senses control pressure and commands down to counteract the pull-up. the pilot pulls harder, exacerbating the problem. the mu-2 is a very clean aircraft and can exceed `never-exceed' speed very fast in a dive from cruise speed. faster than about 115 per cent of this speed, and the aircraft starts to break. speculation is that the pilots don't figure out the problem before they reach these critical speeds. other speculation is that there is a failure mode of runaway nose-down trim caused by the autopilot. even other speculation is that control of the aircraft is coming up against human-factors issues that were (and still are) poorly understood. it's clear that many of the accidents are pilot-induced, as with many very-high-performance planes.

peter ladkin, ladkin@kestrel.arpa

[Late word from Nancy Leveson suggests that the equipment in question is analog rather than digital, but that is still quite computer related... PGN]

Autopilots and conflicting alarms

Matt Jaffe <jaffe@commerce.UCI.EDU>
Thu, 29 Oct 87 12:11:11 -0800

In RISKS 5:51, Joe Morris commented on conflicting alarms in a 727 accident. My aero engineering days are a few years back, but I seem to recall that a stall warning caused by high angle of attack (which translates to a function of [low] indicated airspeed and dynamic load, the product of weight and G-loading, assumed to be close to 1 for an airliner in cruise condition) and overspeed warning caused by Mach number limitations (it is the Mach buffet that is the problem at that point, not the dynamic pressure) occur together at that point in the flight regime so aptly named the "coffin corner". That point, unfortunately, is also the point of maximum specific range, is it not? (Which is why all airlines always try to fly as close to it as possible.)

Several points seem worth noting:

(1) Airline flight crews know about the coffin corner, they fly close to it all the time, do they not? The presence of the two alarms should not be considered as contradictory; they are both correct and indicate an unambiguous situation for which recovery procedures are (or should be) well known.

(2) As to whether the two-alarm condition is confusing, the presence of two alarms that must be interpreted by the human operators (as opposed to a single, "coffin corner" alarm) is a function of the use of analog-mechanical alarm systems. The stall warning system operates (I presume) off of angle of attack; the overspeed warning off of Mach number (pitot differential and temperature). Neither system is connected to the other, the design would be cumbersome, expensive, and risk-inducing. Interpretation of the two-alarm condition is properly (for the analog-mechanical case) left to the human being. The introduction of digital, autopilots offers a chance to improve the situation somewhat. Instead of merely duplicating the set of alarms provided by the older technology devices, good digital system design would add the logic to check for both conditions and then generate a new, unambiguous, "coffin corner" alarm. What is cumbersome and risky for a mechanical system is much easier and hence perhaps appropriate for digital technology. The use of digital computers to detect, interpret, and indicate conditions caused by the interaction of multiple factors is a chance to reduce risk.

Aircraft control systems

Joe Morris (jcmorris@mitre.arpa) <jcmorris@mitre.arpa>
Sat, 31 Oct 87 14:59:11 EST

Matt Jaffe's comments are well taken, but I would like to add a few closing notes:

o His comments about "coffin corner" are correct. From what I've read (no, I'm not a heavy-iron pilot) the best efficiency can generally be found where the Mach buffet meets the stall warning. One mark of a good pilot is the ability to find the best compromise between performance and safety margin.

o The 727 crash I referred to, however, involved a *false* high-speed warning. The cockpit instruments indicated an airspeed of 420 kt at 24,800 feet msl with a rate of climb of 6,500 feet per minute. (not 30,000 feet...my error) This is far above the performance possible for the aircraft. The readings were consistent with the pitot heads becoming blocked as the aircraft climbed through 16,000 feet.

o Finally, the integration of various sources of data to produce situation-specific alarms is not only a good idea, but is being done in various implementations already. (I assume that someone is working on a "coffin corner" warning; I'm not in a position to routinely see such stuff.) the problem is that regardless of the way in which data is processed, the GIGO principle still applies, and the sensors are of necessity still mechanical analog devices. If the primary data source is lying, the user of the data may detect that conflicting information is being received, but it's not always possible to determine which of several sources has failed. The Air Florida crash in Washington is another example of exactly this kind of situation.

Oh yes...from time to time PGN asks for specific citations of incidents. The accident I was citing was Northwest Airlines, Boeing 727-251, N274US, near Teiells, New York, 1 December 1974.

New encryption method

Stevan Milunovic <Milunovic@KL.SRI.Com>
Fri 30 Oct 87 09:13:29-PST

New Method to Protect Privacy of Computerized Data is Patented,
By STACY V. JONES, c. 1987 N.Y. Times News Service, 31 Oct 1987.

WASHINGTON - A professor of computer science at a Virginia college has invented a new method of protecting the privacy of computerized data. He was granted a patent this week for a cryptographic system that he describes as much less time consuming than present methods.

Professor Hito Asai of Christopher Newport College in Newport News received patent 4,703,503 for what he describes as simple mathematic computation, technically known as Vector Boolean algebra. The computer data is enciphered with a long numerical key. According to Asai, an eavesdropper who attacks the enciphered text would face a time-consuming process. He plans to offer licenses to computer and communications manufacturers.

[It may take even less time for the cracker to break, if the long key is stored or transmitted in the clear... Simple numerical algorithms may also be subject to inversion. But this is certainly worth investigating. PGN]

The Stock Market and Program Trading

Dan <db@tcgould.tn.cornell.edu>
Fri, 30 Oct 87 05:15:13 EST

I used to work on an index arbitrage trading desk and I downloaded and executed the baskets of stock orders that Mr. Nelson mentions in the Wall St. Article of Oct. 13, cited a few issues back. He relates a horror story of someone pushing a button over and over after not getting any response and buying $100M instead of $25M worth of stock -- I heard this almost two years ago. Supposedly, the culprit was his printer being offline, and not printing the orders as they were sent down to the exchange. Currently, software distributed to brokerage houses by the NYSE has safeguards against this, such as ignoring input until transmission of a set of orders is complete. (Not everyone uses this software, though.)

We've also seen share volumes of unheard of proportions. One statistic on TV was that there were more shares traded last week than in all of 1965. One explanation for this is the size of the orders allowed on the exchange's computer systems. Until last December, an order through DOT (the system which handles "market" orders) was limited to 2000 shares. Since then, that limit has been raised to 30,000. With the ability to transmit 100 orders per minute, one PC AT has the capability to buy or sell up to 3 million shares per minute. And there are many systems of this type on the street. (Of course, that does not mean that these machines are continuously in use or always dealing in volumes of 30,000 shs/order.)

Are these trades being done completely without human intervention? The answer is no. The program trading most often referred to is index arbitrage. Arbitrage takes advantage off price discrepancies of the same good in different markets, and involves buying the underpriced one and selling the overpriced one. The most common index arbitrage is done on the S&P 500 and its corresponding futures. The futures market at the Chicago Mercantile Exchange still uses open outcry (a la Trading Places) to do business. This means that, although the computer screen may tell you that now is the time to buy stocks and sell futures, you'd better make sure your guy in Chicago did his job and got you a good price on the futures before you push your button and buy $x million worth of stock. There's substantial monetary risk involved, and most (if not all) traders would not surrender that decision to a computer.

The portfolio insurance mentioned a few issues ago deals only in futures, which again means trading via open outcry, and not with computers. Computers are used in this strategy for modeling purposes, to tell the portfolio manager how many futures he should sell to hedge his market exposure.

The only programs I've heard of that may possibly do transactions strictly by computer are AI programs that try to anticipate very short-term trends in the market and buy or sell just before the market moves in that direction. I have not seen these, and don't know how well they work, how widely they are used, or how "automatic" they are.

As far as I can see, it is just the *ability* to move large amounts of money in and out of the market very quickly that has changed things. Computers are still not decision-makers, although they do provide real-time data and much quicker reaction time to that data. But alot can

happen in the five minutes it would take to buy or sell all 500 stocks in the S&P 500. It is the trader who makes the judgement whether the transaction could be profitable or not.

It should be noted that the DOT system was not allowed to be used for index arbitrage programs for the rest of the week after the big drop last Monday (10/19), yet the daily volume was still much higher than had ever been seen before. In addition, the President of the Chicago Mercantile Exchange said that program trading accounted for only about 10% of the volume on the NYSE on 10/19. (New York Times, 10/28, p.D11) I would take this to mean that the programs were not the driving force in the market moves, and that it was real selling.

It is possible to do these transactions without computers, but harder to make them profitable because of the extra time involved when human agents are used, and therefore much less likely that they occurred when using the computers was not allowed. The time windows for the existence of profitable market spreads are often as short as 30 seconds.

One argument defending program trading's market impact on stock prices is that it reflects real selling or buying. S&P 500 futures should trade around their "fair value," which is a premium over the S&P 500 index number based on interest rates and dividend flow. If buying or selling moves the price of the futures too far above or below the fair value, arbitragers can take advantage of this mispricing. But if the price of the futures is pushed below its fair value, it is because people are selling futures instead of stocks. If the futures market weren't there, these people would be selling stocks. It's almost like a simplified Rube Goldberg diagram. Instead of selling stocks directly, you sell futures which causes someone else to sell stocks because you have made them overvalued compared to futures.

Once again, computers are blamed without much real knowledge of the process involved. The conventional wisdom is that program trading is completely automatic, without human intervention. Yet it is the human trader who is in control of the two transactions involved -- one talking to a guy in a futures pit shouting and making strange hand signals, and another typing a few keystrokes at a keyboard.

Dan Blumenthal

db@tcgould.tn.cornell.edu

Program trading (Re: RISKS DIGEST 5.51)

Brent <itm!brent@csl.sri.com>
29 Oct 87 20:48:11 GMT

In light of recent Wall Street instabilities and previous discussion in RISKS about computer voting fraud, some history might be in order.

Thomas Alva Edison's first commercial invention was an electric voting booth. The votes were electrically and instantly tabulated.

Unfortunately, American politics at the time wasn't interested in either fast or accurate vote-counting. The machine was a commercial failure. Edison vowed then and there never to develop a machine that there wasn't a ready market for. His next invention was the ticker-tape.

In light of the ensuing century, perhaps we would have been better off if the response to his machines were reversed :-).

Brent Laminack (gatech!itm!brent)

Minuteman Missiles...

John J. McMahon, STX/COBE x4333 <fasteddy%sdcdcl.span@VLSI.JPL.NASA.GOV>
Thu, 29 Oct 87 13:35:34 PST

WTOP, the local all-news radio station in Washington D.C., reported the following on 28 October 1987. Unfortunately, I was riding along in my car when I heard this, so it isn't verbatim.

3 years ago, at a SAC missile base in the midwest, a Minuteman III missile malfunctioned. The missile was carrying three nuclear warheads, and went into launch mode. Technicians couldn't understand what was going on, since there was no alert occurring at the time. Their immediate reaction was to take a large armored personel carrier (APC) and park it on the missile silo. Assuming the silo doors opened, the APC would fall into the silo, and hopefully stop the missile. Missiles apparently do not arm their payloads until they are off the ground. The report went on to say that the missile did not launch, and that the fault was tracked to a problem in the guidance system. The incident was never reported to the Strategic Air Command, local officials, or apparently anyone outside the missile base.

According to this, the only way we can stop a malfunctioning missile is to drop a big 'rock' on it.

John McMahon, FastEddy@Dftnic.Gsfc.Nasa.Gov (Internet), FastEddy@Iafbit(Bitnet)

Search RISKS using swish-e

Report problems with the web pages to the maintainer

Search RISKS using swish-e

THE RISKS DIGEST

Forum on Risks to the Public in Computers and Related Systems

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

Volume 5: Issue 53

Monday, 2 November 1987

Contents

Re: Risks in intelligent security algorithms (RISKS 5.52)

David Redell <redell@src.dec.com>
Mon, 2 Nov 87 11:10:03 PST

Peter Denning reports (5.52) on an annoying rough edge on the San Francisco Airport's parking lot computer system, which attempted to double charge him when he re-entered the lot on the same day. I had a similar experience at the San Jose airport, but in my case, I parked for two consecutive weekends, and when I left after the second one, the blasted system tried to charge me for the week in between! This seems really unforgivable, since it had plenty of time to both purge the old record and enter the new one. Fortunately, I just happened to still have the first receipt in my car. Unfortunately, I was in a

hurry, and so did not display Peter's diligence in tracking down the official "explanation".

[Sounds like the SAME program! If you drive a BMW, Let the Bayer Beware. PGN]

Danger of typing the wrong password

Scot Wilcoxon <umn-cs!sewilco@datapg.MN.ORG>
1 Nov 87 15:37:22 CST (Sun)

Yet more from the Program Trader Nelson article (WSJ, Oct 13, pg 39):

> One time, a broker typed in the wrong password (on the Bankers Trust computer), which happened to be another broker's password. "So they both had this same list of securities. I get a call from a broker saying, `I'm trying to buy XYZ and it keeps getting bid up out there.` We couldn't figure it out. Then it suddenly dawned on us that (two different brokers) were working the same list."

Both brokers were getting the same list of stocks to buy and sell, and were bidding against each other.

Scot E. Wilcoxon sewilco@DataPg.MN.ORG {ems,meccts}!datapg!sewilco
Data Progress Minneapolis, MN, USA +1 612-825-2607

Inadvertent Launch

<portal!cup.portal!Kenneth_R_Jongsma@Sun.COM>
Mon Nov 2 17:06:28 1987

In regards to the post that talked about parking a vehicle on top of a Minuteman III silo to prevent it's launch: I was a Minuteman commander for several years and had a similar experience. One evening while on alert, I had a missile report "Launch In Process". This was unusual, to say the least! It was also not preceded by the usual indications of a launch. When I called the problem into the base, I received the reply: "Well sir, keep an eye on it. It's either going to launch or shut itself down. In either case, there's not a lot we can do about it." This was not a true statement and probably was the type of Shortly thinking that led to the vehicle being placed over the silo at F.E. Warren. If that did indeed occur, it would be questionable to it's effect. The silo door is approximately 5 feet of hardened concrete and is designed to open even when buried under a substantial amount dirt and rubble.

Inadvertent launch sounds serious, but hold on before you assume the worst. A subsequent investigation revealed that there was a fire in the communications rack that reported site status. At no time were any of the interlocks that prevent accidental launch at risk. In effect, the missle's status had never changed from the reported "Strategic Alert".

I have worked with many systems, I would say that none have the number

and well thought out sets of fail safes for both Type I and II accidental launches. One interesting fact is that no part of the launch *procedure* for Minuteman or MX is classified. Only recently have the operational manuals been restricted to offical use and probably could be obtained under the Freedom of Information Act.

The challenge, of course, is to design, build and test systems that have an acceptable level of risk.

MX Missile guidance computer problems

<ihnp4!ihlpl!jhh@ucbvax.Berkeley.EDU>
Mon, 2 Nov 87 19:44:10 PST

I'm sure many people will have something to say about Sunday's 60 Minutes report about untested parts being used in the MX Missiles currently deployed. I'll refrain from comparing this to SDI, and stick to the story.

There are three variables that make up a project: quality, budget, and schedule. It has been said that it is possible to meet any two of these objectives, but only at the expense of the third. It appears that, in the eyes of lower management, the personal risk of not meeting the schedule was greater than the risk of manufacturing products that had not been fully tested. After all, if the US ever had to use these parts, the individuals are not likely to be around to face the repercussions of MX missiles landing in Chicago rather than Moscow.

Although this particular program focused on untested, but certified falsely as tested, hardware, similar problems exist is software development. Software developers are loath to have someone else checking to be sure that they have done all the work they said they have done. The feeling is that each individual is trustworthy, and checking work exhibits a lack of trust. Unfortunately, human nature is such that someone testing an error leg of code, probably at 2:30 in the morning, is likely to declare themselves done, as they "know" they did a good job coding the software, and the last 20 error legs they tested had no problems. Even worse is the case when their manager is pushing hard to meet a particular schedule, and the project is understaffed. The 60 Minutes program showed how hard it is to use auditors to discover problems when management does not want to know that a problem exists. The organizations telling the auditors what to do all had a vested interest in the project being completed on time.

Any suggestions? John Haller ihnp4!ihlpl!jhh

Re: Autopilots

<research!wolit@ucbvax.Berkeley.EDU>
Mon, 2 Nov 87 06:33:59 PST

Joe Morris is correct in stating that a pilot should be able to overpower a failed autopilot. Of course, fighting a bad autopilot is

not the safest way to fly, either.

While not exactly pertinent here -- most general aviation autopilots are analog, not digital devices, and thus hardly qualify as "computers" by most people's definition -- a few autopilot "war stories" may be of interest.

My friend had flown his Grumman Cheetah (a light, single-engine plane) to a nearby airport for its annual inspection, and the shop offered to have an instructor fly it back to him afterwards. Without shutting down, the instructor slid across to the right seat, and my friend climbed into the left to fly the instructor back. (I know it sounds complicated, but it's a lot easier than setting up a car shuttle.) He immediately noticed that the controls felt much stiffer than usual, and mentioned this to the instructor. The instructor replied that the shop had probably tightened up the control cables, and that everything was normal. My friend took off and flew to the instructor's airport, disturbed that the usual light, responsive control feel of the Grumman had been replaced by the truck-like feel of, say, a Cessna (no flames from Cessna owners, please). After landing, he went to the shop to complain about this. The mechanic came out to the plane, moved the control yoke, and said that it felt fine. My friend tried it and, sure enough, it moved freely. Turned out that the instructor (who usually flew Cessnas) had flown to my friend's airport with the autopilot engaged, and that my friend had not noticed this during the run-up and return flight. The single-axis (roll) autopilot had been engaged in a navigation-aid tracking mode, but the nav radio had been off for the short flight, so the autopilot had been busily trying to hold the ailerons neutral, fortunately without overwhelming success.

The other point I want to raise concerns a particular type of autopilot (or mode of operation) popular on many corporate jets and turboprops and heavier piston twins. This is known as a flight director, and it involves having the autopilot compute the desired flight path for a particular maneuver (a missed approach, e.g.), and display on the artificial horizon -- the primary attitude reference instrument -- a set of "command bars", which direct the pilot to maintain the appropriate aircraft attitude. In other words, the autopilot assumes the "executive" function, and the pilot serves as a servo motor! I never understood why anyone would use such a device. I read a report of an accident several years ago in which a corporate plane -- I believe it was an MU-2, in fact -- took off from National Airport in D.C. and flew into the river for no other reason than that the flight director went psychotic and commanded the pilot to do so. It seems to me that it's hard enough to remain skeptical of what your instruments are telling you and maintain a cross-check on their reliability, without reducing the pilot to the status of a robot, slavishly following George's orders.

Jan Wolitzky, AT&T Bell Labs, Murray Hill, NJ; 201 582-2998; mhuxd!wolit
(Affiliation given for identification purposes only)

---

aircraft accident

Peter Ladkin <ladkin@kestrel.ARPA>
Mon, 2 Nov 87 15:03:53 PDT

i found the following letter in the 8.1.87 copy of aviation safety. apart from the deja vu, it raises questions about certification procedures for light aircraft, does it not? i had understood that aircraft had to be flown through all the appropriate flight regimes to validate the data. maybe i am mistaken, and perhaps someone can clarify?

density-altitude is a term used for the `correction' of true altitude for `non-standard' air temperature (based on the international standard temperatures and lapse rates used for aircraft design). all pilots are taught to compute it, and to be aware of it on takeoff from `hot-and-high' fields. it's a measure of airplane performance, e.g. i have taken off from grand canyon (6606ft MSL) on a hot day in june when the density altitude was 9300 feet and i expect the airplane to behave according to the handbook's figures for 9300ft.

the letter is reprinted without permission. i reproduce the letter in full because of the apparent legal history. the grumman aircraft are not currently in production.

peter ladkin

(From Donald H. Slavik of Milwaukee, Wisconsin)

I enjoyed the article in your May 15, 1987 issue regarding the Grumman AA-1. As an attorney, several years ago, I represented the estate of a man who was killed in an accident involving this aircraft. He attempted to take off from a 3,000-foot long, 150-foot wide, one-degree uphill grass runway in northern Wisconsin. The aircraft was loaded to maximum gross weight and the outside air temperature was about 70 degrees. The aircraft failed to clear trees which were located 1,400 feet past the end of the runway.

My investigation into the background of the aircraft revealed that original flight testing for takeoff and climb performance was accomplished at sea level only. This data was then used as input to a computer program to reduce it to data applicable to higher density altitudes. A careful review of the computer program revealed that there was a sign error in one of the exponents for the critical equations. This caused serious errors in the resulting output data. Secondly, the technical research paper which the computer program was based upon had a footnote which was ignored by the manufacturer of the aircraft. The footnote pointed out that these equations were not applicable to aircraft with low thrust-to-weight ratios (such as this particular plane).

We initiated our own set of flight tests under the direction of Michael Antoniou, the consultant referred to in the Aviation Consumer article. These tests, accomplished at the same density altitude as that which existed on the day of the accident, correctly predicted the performance of the aircraft and also matched the impact point in the trees.

In conclusion, I sincerely believe that the takeoff and climb performance data in the pilot's operating handbook is incorrect.

[End of Letter]

Missiles; predicting disasters

David Chase <acornrc!rbbb@ames.arpa>
Mon, 2 Nov 87 10:13 PST

(on faulty missiles)

I find it interesting that the doors are controlled by the missile and not by the person(s) giving the launch order. I suppose that this removes one way of thwarting a launch, but it seems unlikely that agents of the Evil Enemy Empire would be able to get at the door controls if they were ground-based (certainly, it is no more likely than them being able to park an APC on top of the silo). The trade-offs that our military makes between ensuring a desired launch and preventing an accidental launch tend to give me the creeps.

(on predicting disasters, and the comment that it didn't really matter)

There is no question that disaster prediction is useless without some advance preparation. Since there is a cost to both prediction and preparation, as soon as the expected cost of disaster X falls (well) below the costs of prediction and preparation, one stops preparing and predicting. Consider hurricane preparation on the West Coast, earthquake preparation on the East Coast, and snowstorm preparation in the South. One region's minor disaster is another region's calamity, and a day or two of warning won't help that much. Preparation for all these events requires widespread, long-term preparation, and an occasional "baby disaster" helps enormously to keep people aware and to test their response.

I find the current administration's early depictions of SDI particularly amusing in light of this. Remember the "umbrella"? Whatever happened to civil defense? I recall some interpretation of civil defense as "threatening" -- does that mean that SDI is not? On the other hand, civil defense may whip up emotions in ways that the "umbrella" does not; it's harder to generate public sentiment for peace and friendship when the public is also preparing for an attack by the Evil Enemy Empire. Sigh. I wish I could think that this was Reagan's Secret Plan for better relations with Russia.

David

DISCOVER Uncovered?

<BNBaker@KL.SRI.Com>
Mon 2 Nov 87 14:44:51-PST

I just received a promotional letter designed to entice me to join Discover Card Travel Services. There is a sweepstakes involved in which I may already

be a winner. I get so excited everytime I read those words. In other words, I get excited at least once a day, but this one has a new twist.

The flyer states, "Enter now. You could be an INSTANT WINNER! Your dream vacation stamp bears a unique UPC Symbol. It will be electronically scanned to reveal if you are an instant winner!" It so happens that we have two Discover cards for some reason, and I happened to open both envelopes. I already mentioned how excited I get and so I was able to get excited twice. Then I noticed that the UPC symbols were the same on both flyers. As you may recall from a couple of issues ago, I have an interest in semantics so I called Discover Card to learn about this new meaning of the word "unique." I was told that there is a secret code on the UPC Symbol that makes each one unique. The bar codes are identical so there would have to be some special material in the ink of the winning ones. If, however, the bar codes differed on the winners, then the winners would be obvious to those printing them up. Either way, my entries are not unique, as claimed. The Discover Card representative simply gave cute answers back to my questions.

They asked how big my sample size was, so part of the purpose of this is to ask RISKS readers if they by chance received the same unique set of UPC symbols that I did, namely Canada 12345 06240, Hawaii 12345 50030, West Germany 12345 02990, Walt Disney World 12345 75740, Colorado 12345 00580, Arizona 12345 10300 If yours are different, please let me know also.

The things that annoy me about this are:

> The aura of electronically scanning the entries to determine who the winners are, when in fact that process may not take place.
>
> The attempt to dispense my concerns by stating that there is a secret code on each of the UPC symbols that can only be read by their special computer.

The technology is produced by UPC Games of Chicago (no phone listing). At a minimum, this appears to be misrepresentation, but I've been notified that I may already be a winner so many times that this slight twist to the misrepresentation game should not bother me I suppose. Does anyone know how this one supposedly works?

Bruce N. Baker <bnbaker@kl.sri.com>

TV Clipping Services

<"Tom Benson 814-238-5277" <T3B@PSUVM> [BITNET]>
Sun, 1 Nov 87 08:33 EST

In RISKS-5.51 Will Martin asks about TV clipping services. The best comprehensive source for network television news is the Vanderbilt Television News Archive, at Vanderbilt University. They collect all national network news (since 1968, I believe), plus some special events. Full print indexes of this service are available at good research libraries or from Vanderbilt. They will provide videotape of specified stories at, I believe, about $100 per hour of tape.

There are also several commercial clipping services, which charge more but which also collect such things as local tv news. They operate in several major cities, but I have little information about them; I could find out more if it's of interest.

On the general point, Will is right: these services are a good way to monitor what the public is hearing about various areas in which scholars and scientists are interested.

Tom Benson, Penn State University [Also noted by Charles Youman]

Video Clips

Samuel B. Bassett <amdcad!well!samlb@hplabs.HP.COM>
Fri, 30 Oct 87 23:29:39 PST

For the person wondering about being able to get videotapes of TV programs, I would suggest contacting Bacon's PR & Media Information Services in Chicago. They do, certainly do newspaper and magazine clips, and may also do video clips -- if not, they will likely be willing and able to refer you to somewhere that can.

The address and telephone number I have are from 1984, but they do have an '800' number, and you can get it by dialing 1-800-555-1212 and asking the AT&T operator.

Bacon's is a decidedly commercial operation, and is not cheap, but my experiences with them in '81-'83 were decidedly positive.

Search RISKS using swish-e

THE RISKS DIGEST

Forum on Risks to the Public in Computers and Related Systems

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

Volume 5: Issue 54

Wednesday, 4 November 1987

Contents

Erroneous $1M overdraft -- plus interest

Dave Horsfall <munnari!astra.necisa.oz.au!dave@uunet.UU.NET>
4 Nov 87 13:13:34 +1100 (Wed)

From the Sydney Sun-Herald, 19th October 1987:

``The bank manager panicked when he saw the size of Brian Jamieson's overdraft - all $100 million of it! To add to the horror, an additional $53,000 interest debt was accruing daily on the account.

But Mr Jamieson ... was the last to panic, thanks to a frantic telephone call from his Westpac bank manager who told him to take no notice of any statement - it was all a mistake. [...]

The bank manager said he was not sure how the error had occurred. "Something happened with the computer and it went through" he said. [...]

Curiosity has since got the better of Mr Jamieson. He has requested a copy of the offending bank statement so he can frame it.

Dave Horsfall (VK2KFU) ACS: dave@astra.necisa.OZ.AU
NEC Information Systems Aust. ARPA: dave%astra.necisa.OZ.AU@uunet.UU.NET
3rd Floor, 99 Nicholson St UUCP: {enea,hplabs,mcvax,uunet,ukc}!\
St. Leonards NSW 2064 AUSTRALIA munnari!astra.necisa.OZ.AU!dave

Wrongful Traffic Tickets & Changing Computers

"David A. Honig" <honig@CIP.UCI.EDU>
Mon, 02 Nov 87 11:50:02 -0800

A month ago, I received a notice stating that I had two outstanding parking tickets (delivered on successive days) for violations occuring in UC Irvine parking lots, and that if I didn't pay over $100 I would have a warrant out for my arrest. As I didn't know about the tickets, I made some phone calls and was told to send the tickets to the Parking & Transportation office here.

Today I called them to find out what my status was. I told them the date of the citation, and was told "just to trash them". They claimed it was a "computer error". I asked them for more details: they had "changed computer companies" and the new system had different codes, causing paid tickets look unpaid and vice-versa, and confusing other information besides (apparently including sending out tickets to the wrong people). The person on the phone told me that they had to erase three month's worth of tapes due to these problems.

Weather -- or not to blame the computer?

Stephen Colwill <mcvax!praxis!steve@uunet.UU.NET>
Mon, 2 Nov 87 13:17:35 BST

I would like to make some observations on the subject of the recent storm.

The remarks about mesoscale weather systems seem to be relevant though I was under the impression that the model used by the Met Office took into account surface features (mountains etc) so it cannot be completely restricted to high altitude (and therefore large-scale) effects.

The paucity of weather stations in the sea is a difficulty that the forecasters have to live with, almost all the weather that England has builds over the Atlantic and it seems to me that ships caught in a system like that are going to have more problems to deal with then relaying detailed data on the atmospheric conditions to the mainland. This situation is distinct from those countries with a continental weather pattern and poses more problems for the modellers.

Another point worth noting is that in this country we are not really "geared up" to such unusual weather, whenever there are severe snowstorms for example the parts of the country affected are generally brought to a complete standstill. In America, on the other hand, a whole infrastructure exists for closely monitoring the progress of hurricanes etc, and the people are prepared

(as far as they can be) for them.

On the storm itself, it seems to have followed a rather peculiar path of evolution. As I understand from the subsequent reports it started as two centres of depression which amalgamated suddenly in the Bay of Biscay. After this point it reached its unprecedented violence, up to this point the depressions would have been on the nasty side of normal. These depressions were fuelled by colliding air masses which had a high temperature difference. Any model which could have predicted *that* gets *my* respect. In its new state the storm was so energetic that (on the scale of the Paris-London distance) it could have gone anywhere and only swung over the SE of England at the last moment.

A consequence of the storm was that the power loss in the SE significantly disrupted network communication overseas since ukc (I guess) had some power outages.

In my opinion, these observations completely exonerate the model-makers and their machines. If this storm had been predicted there would have been a good case, on the other hand, for their extensive congratulation.

There is a body of thought that has it that such violent weather is on the increase as the average land-sea temperature difference increases (the greenhouse effect apparently) so it seems that computer models will have to get to grips with it eventually :-)

Steve Colwill, Praxis, Bath, England.

Re: Computer's Normal Operation Delays Royal Visit

<mnetor!utzoo!henry@uunet.UU.NET>
Tue, 3 Nov 87 13:59:08 EST

> ... As the royal party was early, the control room dispatched
> the train manually rather than keep Her Majesty waiting for five minutes.

It's noteworthy that this means that the ultimate cause of the foulup was elsewhere. The royal party is not supposed to arrive early. One reason why the Queen's Flight aircraft always carry navigators (not normally found on civil aircraft nowadays) is that their arrivals must be precisely on time -- neither late *nor* early.

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

Auto-pilot Problems and Hardware Reliability

Craig Johnson <vince@tc.fluke.COM>
Tue, 3 Nov 87 10:55:01 PST

The discussion about alleged auto-pilot failures has reminded me of a discovery I made a few years ago with regard to hardware reliability

which has serious implications for many applications and may certainly be a risk to many people.

I was involved at the time with a design which used a very common, inexpensive single-chip processor made by a major manufacturer. My application was such that I was able to observe the behavior of this processor when very frequently reset with an asynchronous signal, on the order of 10-50 times a second. Even though the manufacture's literature claimed that the reset input was asynchronous and even had schmitt-trigger-like conditioning, much to my consternation I found that once every few minutes the processor would go crazy and my system would hang.

After much hair pulling and careful scrutiny, I found that indeed once in a great while a reset would fail to properly initialize the processor and the thing would actually start fetching code at some bogus address rather than at its reset address. The failure was duplicated with several different processor chips, confirming that the behavior was a characteristic of that processor. Synchronizing the reset signal to the bus cycle completely cured the problem and it was never seen again.

It may be conjecture, but my conclusion was that this was a classic case of meta-stable states in flip-flops. Regardless of the schmitt-trigger conditioning, there was an internal latch which was supposed to sample the reset input which if clocked at just the right moment during the transition of the reset signal would go meta-stable, "balanced" between states and slow to "fall" to a valid state. When the transition was too slow, incorrect and incomplete processor initialization would take place.

I felt fortunate to have discovered this flaw in the processor behavior before my application went to market. I have often wondered how many other systems out there suffer from the same kind of flaw and are prone to unexplained failures "one in a thousand" times.

Minuteman III (RISKS-5.53)

Bryce Nesbitt <bryce%hoser.Berkeley.EDU@Berkeley.EDU>
Wed, 4 Nov 87 00:46:19 PST

>RISKS-LIST: RISKS-FORUM Digest Monday, 2 November 1987 Volume 5 : Issue 53
>
>In regards to the post that talked about parking a vehicle on top of a
>Minuteman III silo to prevent it's launch...
>...If that did indeed occur, it would be questionable
>to it's effect. The silo door is approximately 5 feet of hardened
>concrete and is designed to open even when buried under a substantial
>amount dirt and rubble.

The local journal of mis-information claims that the truck was parked oriented in the direction of door opening with the brakes

off. The theory was that the "rug", so to speak, would be pulled out from under the vehicle which would drop and damage the missile.

The net result might range from launch failure, to fireball, to local radioactive contamination (or even local detonation, just possibly). Any of those alternatives would be better than dropping a nuke on some *other* country.

Rather than just spread this rumor, I'd rather hear from someone who knows about how this silo door is designed to keep "a substantial amount of dirt and rubble" from falling into the silo.

Assume the contingency that the silo commanders must have faced... an electrical malfunction that they felt *might* cause an unintended launch, no matter how unreasonable you may think that is.

[Marginally relevant, but it has intriguing systems implications!

Bryce's subtle comment of appending the results -- which I have omitted here -- of a spelling corrector applied to RISKS-5.53 suggests that the spelling in that issue was execrable. (And of course his spelling corrector missed the two "it's" above.) In case you haven't noticed, I have eased up somewhat in trying to correct contributed typos and grammatical horrors. (It should reflect on the author, not on me?) But I certainly echo the implied grumble that the contributed writings are getting sloppy. I try not to squelch an interesting contribution just because of its writing, but please remember the word "coherent" in the masthead. PGN]

Search RISKS using swish-e

Report problems with the web pages to the maintainer

Search RISKS using swish-e

THE RISKS DIGEST

Forum on Risks to the Public in Computers and Related Systems

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

Volume 5: Issue 55

Thursday, 5 November 1987

Contents

Phone prefix change cuts BBN off from world

<dkovar@VAX.BBN.COM>
Thu, 05 Nov 87 15:46:11 -0500

On the first of November, BBN in Cambridge MA acquired a new prefix to replace it's three old prefixes. Any calls to the old numbers were supposed to get a message informing the caller of the new number. Standard stuff. Well, perhaps not quite. The following messages were culled from the corporate bboard. Corporate and personal risks abound. "Has BBN gone out of business?" "Oh, you gave us a false work number, that's grounds for a lawsuit." "I've been trying to reach you all day to inform you that ....".

-David Kovar

I have been having problems with people reaching me at my new 873 number.
It turn out that this seems not to be a fault of the tel company or our PBX
but not-up-to-date data-base of phone exchanges in the caller's PBX. The 873
extension is new to Cambridge! An interesting distributed data-base problem..

As noted in an earlier bboard posting, BBN's new number has to be distributed
to a lot of telephone switches. Errors in the distribution can be fixed, but
only if the BBN folks in charge of voice communications get involved. So, if
you learn that anyone is having trouble calling BBN, it would be helpful if
you would report this to Curt D'Aguanno (ext. 3845, email "cdaguanno"); he
will need to know where the caller is calling from, and what carrier they
are using (AT&T, MCI, ...) if you know.

Please note that the distribution of our new number is really outside of
BBN's control; all Curt can do is report the problem to the carrier in an
"official" way and keep after the carrier to fix the problem.

NOT ONLY DO SOME NUMBERS NOT WORK, BUT WHEN YOU CALL THE OLD NUMBERS,
THE RECORDING SAYS THAT THE NUMBER IS OUT OF SERVICE, CALL YOUR
OPERATOR FOR HELP. I CALLED HER, SHE SAID CALL INFORMATION FOR THE
NEW NUMBER. INFORMATION SAID CALL SOMEONE ELSE,...
IN OTHER WORDS, IF SOMEONE YOU KNOW TRYS TO CALL YOU AT YOUR OLD
NUMBER, TOO BAD!

My daughter's school has been trying to call me all day to tell me she is
very sick. But anyone who tries a 497 BBN number gets a NOT IN SERVICE
message, and calling Information gets no information. Help! Is something
being done about this, hopefully VERY quickly? It's difficult to imagine
how much BBN is losing every hour. I just called a client who said he'd been
trying to reach me since this morning and wondered when BBN had gone out of
business.

A simple application of Murphy's Law

"ZZASSGL" <ZZASSGL@CMS.UMRCC.AC.UK>
Thu, 05 Nov 87 11:43:14 GMT

I look forward to reading all the various complicated ways in which computers
can screw up your life in this forum. There are however some very simple
examples of Murphys Law. The following has just happened to me AND I AM ANGRY!

We received on Tuesday a tape from Purdue University (I mention this because
I'm in Manchester, England). This tape I entered into our "Stranger Tape"
system where it was allocated a tape number and two big sticky labels were
placed on the reel showing the tape number to anybody who cared to read
them. The tape is then placed into the tape racks. I successfully read all
the data from the tape. Today, Thursday, I realize that there are in fact
some corruptions in one of the files that I read. So I attempt to re-read
the file from the tape. This turns out to be impossible because sometime on
Wednesday an operator misread the tape number on the big sticky labels and

mounted my tape instead of the correct one and wrote someone's files onto it.

This occurred on a MVS system and the tape contained a standard label. When you attempt to overwrite a labeled tape on our system an operator message appears asking if you really want to write to the tape. The operator must have answered yes to this question.

This is of course an example of the seeing, hearing, reading what you expect to see, hear or read rather than what is actually there. There appears to be nothing that you can do to prevent this kind of error. The system had correctly diagnosed that there was a problem of some sort and asked for assistance to resolve the matter. It was told to carry on and write to the file.

The consequences of this little screwup are: I may have to request a new tape to be sent from Purdue (24 dollars postage a time); I now have access to someone's files as the physical tape is still registered to me and I can remove it from the tape library by returning the receipt; someone has lost their files without any evidence to show why.

Geoff Lane, University of Manchester Regional Computer Centre

---

Wrongful Accusations; Weather (RISKS-5.54)

<willis@rand-unix.ARPA>
Thu, 05 Nov 87 09:32:01 PST

RE: Wrongful Traffic Tickets & Changing Computers (David A. Honig)

It's OK to have someone tell you over the phone to ignore some allegedly wrongful action of a computer-based system. But do you trust the phone message? And do you trust the person telling you the message? And do you believe that the person indeed knows the correct and complete facts?

At one time I was suspected of fraudulently using my bank card. After it got straightened out, I insisted on an explanation. It took two letters to the bank president to get it.

Turns out that the bank issued both MC and VISA cards, and -- get this -- used the same numerical identification sequences for both. I had a VISA; an MC card of the same number had been lost and fraudulently used. A data entry clerk goofed on the digits which distinguish an MC from a VISA and I got in the barrel.

Through my insistence on an explanation, the bank took corrective action to avoid future similar problems.

For events beyond some threshold, the potential consequences of some action alleged to be wrong are too RISKy to depend on phone notification. It's your individual call when to insist on a written verification, but my personal threshold is very low. Only for the most trivial of events will I accept phone statements.

Willis H. Ware, Santa Monica, CA

- -

RE: Weather -- or not to blame the computer? (Stephen Colwill)

Just a few other comments to wrap the subject up. Maybe SE Britain isn't geared up for serious weather, but neither is the U.S. in some ways. In spite of best efforts, we often screw it up. Example: as a result of a forecast that indicated only light snow, the Washington (D.C.) government delayed calling out the snow equipment for an hour or so. The snow was heavy, not light, and the city came to a half.

Also turns out that the most critical forecast that the NOAA Severe Weather Forecast Center (in the midwest somewhere) has to make for a hurricane is prediction of its landfall location. It's a tricky judgment, and the WX folks try to get the best and continuous data on the storm. But since the on-shore preparation time is measured in hours, the storm can dance around considerably in the last few hours and hence we have the occasional situation of prepared areas not being hit and unprepared areas, clobbered.

Re weather data over the North Atlantic, NOAA experimented a few years back with a package that flew in the hold of trans-Atlantic aircraft and continuously reported weather observations at jet altitudes through the GOES satellite back to Suitland, Maryland. As I recall the argument, the weight of the package cost the airline the revenue of one passenger seat (maybe it was two or three seats) so the experiment was short-lived. I do not know its present status.

Willis H. Ware, Santa Monica, CA

Weather and expecting the unexpected

<EDMONDSON@COMP-V1.BHAM.AC.UK>
5-NOV-1987 12:33:37

It is worth commenting on Stephen Colwill's comment that in the USA everyone is geared up to watch the weather, respond appropriately, or better still anticipate, and in any case their larger land mass makes weather prediction easier.... which I take to be the drift of his contribution.

The winter of '82 will be remembered by inhabitants of Minnesota. Just after Christmas the airport was closed (for nearly 24 hours, first time in 20 years, if my memory serves me well) - by a freak, and unforecasted, snow fall. Not just a few flakes, you understand - Minnesota folk are hardy stock - but more than a foot of snow in a few hours, in the middle of the night.

I know, because I couldn't get back to Minneapolis, and when I did everyone expressed surprise at being caught out, etc. Note that Minneapolis has/had the advantage of the KSTP weather-desk in addition to any national forecasts,

and that Minneapolis is just about centrally located in a huge land-mass.
The Norwegian bachelor farmers no doubt munched on their powder-milk biscuits,
but everyone else felt let down.

I add this to the debate because the usual British arguments - we don't
suffer extremes frequently enough (the usual complaint of railway service
when the points (switches) freeze, as they do most winters), we're too small
for good predictions, etc., just don't add up.

The moral - and comments welcomed on this - would surely be something along
the lines of: people are not psychologically prepared for extremes, of any
sort, and thus don't countenance them readily. What this means for RISKS
is that we (designers of expert systems, or autopilots, or...) need to be
aware that it is at the margins of human experience that our experience
fails us! We're least able to contribute the design data for those areas
of performance where they are most needed.

OK so someone is going to bring up Three Mile Island - fine - but note that
I'm note restricting my comments to simple monitoring failures, or to pressures
of time, etc. A fly or two on the Met. Office walls may well have heard
comments to the effect that 'this looks like a hurricane - but surely not
here' or some such. Does anyone know of observational or other studies on
this aspect of human behaviour - it is particularly relevant to understanding
human response to data provided by computers when those data are unusual,
and thus potentially a component in a risky situation?

> [Readers may recall our mention of the notion of Henry Petroski
> ("To Err is Human") that we tend no to learn from our successes,
> but have a great opportunity to learn from our failures. PGN]

UNIX setuid nasty -- Watch your pathnames

Stephen Russell <munnari!basser.cs.su.oz.au!steve@uunet.UU.NET>
5 Nov 87 02:10:40 GMT

A major security bug in our student assignment submission system was exposed
recently. This system, which allows students to submit solutions for
selected assignments, consists of two programs. The first checks that
the assignment is current, etc., then constructs the file pathnames for
the student's file and the destination (in the appropriate directory for
that assignment). It then invokes the second program, which is basically
a setuid root file copy program. It needs to be setuid root, as it writes
into a protected directory. The copy program is publicly executable, although
(we believed) reasonably well hidden.

Now for the bug. The copy program attempts to prevent incorrect use,
by checking that the pathname for the destination begins with
"/user1/bags/GIVE/", which is the standard place for putting assignments.
However, _it checks no more than that_. It didn't take too long for
some students to discover that "/user1/bags/GIVE/../../.." was also
acceptable. This allowed them to `back up' out of the correct directory to
the root directory, and from there to anywhere they liked!

Thus, they had a program that allowed them to read or overwrite any file on the system. You can imagine the consequences - modified password file, trojan horses installed in various system utilities, etc. When we finally discovered this, it took many, many hours to clean up the mess. Worst of all, we cannot be 100% sure we haven't missed something.

Moral: breaking normal security to provide a needed feature is a risk.

Penetrations of Commercial Systems

<TMPLee@DOCKMASTER.ARPA>
Fri, 30 Oct 87 14:18 EST

Does anyone know if there exists, apart from Donn Parker's publications, any compendium of recent (last ten years) cases of theft, fraud, or unauthorized disclosure, modification, or destruction of information in commercial computer systems (analogous government ones OK too) wherein it is at least plausible that better computer security would have prevented, or helped detect (sooner?) the incident? (I'm also aware of PGN's lists too, of course.) ("better computer security" means technical measures, except for pure physical security and communications security, if weaknesses in those was only exploited in a direct attack on the end information -- if they were exploited as part of an indirect attack (e.g., stealing a password, planting modified software) that would be of interest.)

(Individual reports also welcome; don't send them directly to either forum.)

Ted

Re: Penetrations of Commercial Systems

Peter G. Neumann <Neumann@KL.SRI.Com>
Sat 31 Oct 87 15:51:12-PST

Ted, I presume you are fishing for justifications for better system security and network security in the face of many people trying to argue that most breakins are not the result of poor system security, but rather weaknesses in the administrative, operational, and user practice. That argument needs attacking. Having better systems with more humane interfaces and with nonbypassable and nontamperable auditing could help to diminish the sloppy practice. But having a system with inadequate security and integrity means that the audit trails -- and indeed some of the system controls themselves -- can be readily compromised. Also, many of the external breakins and internal misuses have been inspired by system weaknesses -- even if they resulted directly from sloppy practice.

One particularly horrible case involved administratively turning off the audit trail in order to permit the computer systems to cope with the backlog:

$H Removal of Wall St audit trail enables $28.8M computer fraud (SEN 12 4)

But suitably efficient, nonbypassable, and nontamperable audit trails are included under the notion of adequate security controls; certain minimum level of auditing should not be possible to turn off.

Following are just a few cases in which better system security controls might have helped (including sounder operating systems, better enforcment of separation of privileges in system use and application design, better user identification and authentication, better audit trails and real-time analysis, etc.):

SH Stanford network breakins (SEN 11 5)
SH Crackers break into AT&T computer systems (SEN 12 4)
SH W.German crackers plant Trojan horses, attack NASA, DoE systems (SEN 12 4)
SH Various other Trojan horses (SEN 12 4, etc.)
$H Volkswagen lost $260M, computer tampering foreign-exchange fraud (SEN 12 2)
$SH Phone credit-card numbers stolen from computer. $500M total? (SEN 12 3)
$H N-step reinsurance cycle; software checked for N=1 and 2 only (SEN 10 5)
[although this would have required application-level integrity controls]
$SH 18 arrested for altering cellular mobile phones for free calls (SEN 12 2)

(SEN References are to Software Engineering Notes. Most of these also appeared in RISKS on-line.)

There are lots more cases. These are just a few to get you started. Peter

---

Re: Unix password encryption, again?

Dan Hoey <hoey@nrl-aic.ARPA>
5 Nov 1987 11:39:10 EST (Thu)

In Risks 5.48, Russ Housley asks whether Unix's ``modified DES'' is a one-way hash. Let us first pick nits: he was not asking this of the modified DES per se, but of the Unix password mapping algorithm. The DES and modified DES are cryptosystems, while the password mapping is a transformation from the user's password to an ``encrypted'' version. Confusion arises because the password mapping algorithm uses the modified DES as a subroutine, so there is a strong temptation to say that the password has been ``encrypted by the modified DES''. This usage of the term ``encrypt'' is at odds with the common cryptological concept of a transformation by which information is transformed for later decryption by a secret algorithm, or an algorithm that uses a secret key.

A second point of terminology concerns the term ``one-way hash'', which has been interpreted in four different ways by me and the three people I have discussed it with in private communication. Russ Housley used the term for the composition of a hash function and a one-way function. (A ``hash'' function is a function that maps a large domain to a smaller range. A ``one-way'' function is a function that is computationally infeasible to invert.) When Matt Bishop (Risks 5.49) answered that the password mapping was not a one-way hash, he was referring to the fact

that the password mapping is not a good hash function--the only hashing that goes on is ignoring all but the first eight characters. Peter Neumann interpreted ``one-way'' as referring to a function that maps many-to-one (a reading invited by the term ``hash''). Certainly, it is impossible in a sense to invert a many-to-one function F, since X cannot be determined from F(X). My understanding of a one-way function is one for which it is hard to find any X' for which F(X')=F(X). Such a function can be either many-to-one or one-to-one; I suspect that the password mapping is many-to-one even on eight-character passwords.

So, in answer to Russ's question, the password mapping is designed to be a one-way function, but we have no proof that it succeeds. In a practical sense, no one knows whether the password function is hard to invert, though no one has reported an easy way. In a theoretical sense, if P=NP (and perhaps if not) then no one-way functions exist.

But even if the password mapping algorithm is a one-way function, it is not very secure. Any one-way function can be broken by trying all of the possible inputs. In his message, Matt illustrated this with an example of 100 users who chose passwords from a 25,000-word dictionary. He described the effect of the modified DES, noting that a search for the passwords would require 2,500,000 password mappings, and concluded that ``the time for such a search should be unacceptably high.''

In a later private communication, he clarified this. The example he gave was intended only to describe the purpose of the modification to DES, and not to claim that 2,500,000 password mappings are a serious barrier to password breaking. You might not realize that if you use the software distributed with Unix, which would require ten days for the task on a SUN 3. But last year, Robert W. Baldwin announced a way of speeding up the password mapping by a factor of 300, using VAX assembler code and some tricks. Using his tricks and some of my own, I wrote a fairly fast password mapping in C, and in fact Matt Bishop has his own fast C implementation. So those 2,500,000 mappings can be undertaken by Matt on his SUN 3 in about eight hours, or by Bob on his VAX 8600 in about forty minutes. And if Rick Gumpertz is still out there with his Cray, carry a laser.

The clear and present risk to a Unix system is that the users may have chosen passwords that can be found in a list of words, of words spelled backwards, of first names, of the first letters of famous quotations, of possible license plate numbers, of the six-letter strings, of the eight-digit strings, of the geometrical keyboard patterns, or any other fairly short machine-accessible list.

I am horrified at the amount of verbiage it takes to straighten out these simple misunderstandings. If you want to know more about the issues, read Morris and Thompson's ``Password Security: A Case History'' in the November 1979 CACM or your Unix Manual Set (volume 2, or System Manager's Manual, depending on how your set is organized). Please do not court the wrath of the S. P. F. D. H. by further flogging this dead horse, or me.

Dan Hoey

[This message is the result of extensive trialogue among Dan, Matt

Bishop, and PGN. There were enough confusions exhibited by other readers in other messages -- including a bunch which have not been included in RISKS -- that it seemed worthwhile to try to set the record straight. I hope this won't lead to further confusion. PGN]

Software Testing

Danny Padwa <padwa%harvsc3@harvard.harvard.edu2>
Thu, 5 Nov 87 15:53:39 est

John Haller mentioned the question of software testing an issue or two ago. Last summer I worked at a financial information company which (for obvious reasons) takes software reliability very seriously. They had a testing system, which, although sometimes tedious, seems to work extremely well.

When the development group is ready with a software release, they forward it to the quality assurace group, puts it up on a test system and tries very hard to break it (i.e. we simulated market conditions that make "Blue Monday" look like nothing). Very detailed test plans are written and carried out, testing all sorts of possible failures.

When the QA group signs off on it (often after a few trips back to development for tuning) a software package goes to the Operations Testing Group, which runs it on a test string exactly the way it would run after release. If it is consistent with currently operating systems for about a week, it is then released to the operations teams.

While this is not a sure-fire solution, it does make reasonably sure that any software that goes "live" can handle normal conditions (the Ops testing) and weird ones as well.

Does anyone out there have similar experiences with multiple-redundancy in testing. (NOTE: The various testing groups are relatively well separated administratively, so that pressure on one group usually is not paralleled by pressure on another.

Danny Padwa, Harvard University

BITnet: PADWA@HARVSC3.BITNET HEPnet/SPAN: 58871::PADWA (node HUSC3)
MFEnet: PADWA@MFE.MFENET UUCP: ...harvard!husc4!padwa

38 Matthews Hall, Harvard University, Cambridge MA 02138 USA

Risks of using mailing lists

Dave Horsfall <munnari!astra.necisa.oz.au!dave@uunet.UU.NET>
5 Nov 87 13:20:19 +1100 (Thu)

Quoted from the Sydney Morning Herald, 19 Oct 87:

``An Albion Park [Sydney suburb] reader didn't have to open the letter from a Sydney computer software company to know the status

of his account. On the envelope, between his name and address, was printed: "35 days UNFINANCIAL".''

Obviously, the billing software merely took the data base details as a mailing list label...

-- Dave

Search RISKS using swish-e

THE RISKS DIGEST

Forum on Risks to the Public in Computers and Related Systems

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

Volume 5: Issue 56

Monday, 9 November 1987

Contents

News article on EMI affecting Black Hawk helicopter

John Woods <jfw@EDDIE.MIT.EDU2>
Sun, 8 Nov 87 20:18:27 EST

(Well, after the reports of the President's plane affecting people's garage doors, I guess it is appropriate that we are able to return the "favor"...)

Radio waves reportedly can down copter
By Mark Thompson, Knight-Ridder Service
(From the Boston Globe, 8 November 1987)

WASHINGTON - The Army's most advanced helicopter to carry troops into battle can be knocked out of the sky by routine radio waves from microwave towers, radio antennas, and radars, according to Pentagon officials and documents.

Investigators believe such radio waves made five of the Army's UH-60 Black Hawks nosedive into the ground since 1982, killing 22 servicemen. The problem could be even more devastating in wartime, they said, because the Soviets are perfecting a radio-wave weapon to exploit the vulnerability.

"We've got a very sophisticated electronic aircraft, and if the radiation we're putting up in peacetime -- microwaves, antennas, TVs -- is causing the aircraft to flutter and wobble, then -- and I don't like to talk about this because it is kind of a breach of security -- we're going to have problems in wartime," said Jerry A. McVey, a former Army major who led the investigation into a still-unexplained Black Hawk crash last year.

Radio waves in the air can enter the helicopter's wiring and electrical components and generate false commands that can range from simply flashing the warning lights to sending the craft into a fatal dive.

The Army recently warned its Black Hawk pilots that flight near radio towers can cause unexpected dives that could endanger the $6 million aircraft. "Pilots should be made aware that flights near microwave antennas or shipboard radar may cause uncommanded attitude changes," the Army told its pilots in August following extensive tests earlier this year.

But despite such warnings, the Army maintains there is no safety problem. "None of the anomalies encountered during these tests resulted in control movements causing flight safety critical conditions," the Black Hawk's management office said in a videotaped briefing for the pilots.

A three-month investigation by Knight-Ridder has found:

* The Army grounded all UH-60s last year after one crashed near a high-powered citizens' band transmitter in Alabama, killing all three servicemen aboard. But Army aviation officials ordered the copters back in the air 49 days later without telling pilots -- or the Army's top general -- that the service's safety experts believed there was a 50 percent chance of a similar accident within a year.

* In five mysterious accidents, the Black Hawks were flying below 1,000 feet when they suddenly dove straight into the ground, killing everyone aboard. While the Army listed mechanical causes for three of the crashes, senior Army investigators say they believe radio waves, called electro-magnetic interference (EMI), were the real culprits. The other two crashes are officially unsolved, although investigators suspect EMI.

* While the Army minimizes the Black Hawk's vulnerability to radio waves, the Navy, which also uses the aircraft, has taken a far different approach. The Navy barred its first 14 Black Hawks -- bought for training purposes in 1982 -- from coming within "a significant number of miles" of radio towers for fear of accidents, a senior Navy engineer said. The precise distance is classified. The Navy later demanded that its future Black Hawks, known as Sea Hawks, be heavily shielded from electronic interference. They can now buzz radio towers with impunity.

Officials as Sikorsky Aircraft Co., which builds the helicopters for

both services, said they deliver aircraft shielded to each service's requirements, but declined to comment on the adequacy of the Army's standards.

Because EMI leaves no "fingerprints," the Army has been unable or unwilling to cite it as a cause of any of the 29 Black Hawk accidents that have killed 48 servicemen since 1980. Shielding the Army Black Hawks to Navy standards would be "very costly," Army officials said.

Many of the military officials, pilots, engineers and investigators interviewed in the investigation of the Black Hawk agreed to speak only on condition that their names would not be used. Most of these sources are in sensitive positions and said they could lose their jobs or face disciplinary action if they are identified.

But they speak with certainty about EMI's dangers.

"EMI is causing these aircraft to flip upside down and crash and kill everybody on board," said one senior Army aviator. "There is a definite problem with the Black Hawk and EMI -- no question about it."

EMI is most deadly when it tinkers with the Black Hawk's movable rear wing and its crucial hydraulic system. Both are operated by minute electric signals that can be overwhelmed by outside electronic interference.

A New Twist with Cellular Phones

Leo 'Bols Ewhac' Schwab <hpscda!hpscdl!hplabs!well!ewhac@seismo.CSS.GOV>
6 Nov 87 10:21:29 GMT

Related to me by my father:

My uncle, who operates a mobile comminucations shop (CB's, car stereos, and such) was asked to install a cellular phone into a Pontiac Fiero. When it came time to install the antenna, he wondered if it was kosher to install it on the rear hood, where the engine is located. As I recall, the antenna runs at 800 MHz.

He called Pontiac. After wading through a bit of bureaucracy, he got a technician on the line. The tech said that installing a cellular phone antenna in that position would cause bad things to happen to the electronic fuel injection. He didn't specify what sort of bad things.

It seems to me that, if the electronic fuel injection were properly shielded, this problem wouldn't exist. It also seems to me that proper shielding is trivial. Am I missing something? Is Pontiac missing something?

Leo L. Schwab

Computers Amplify Black Monday

Bjorn Freeman-Benson <bnfb@june.cs.washington.edu>
Mon, 09 Nov 87 08:18:54 PST

In the article "Computers Amplify Black Monday", _Science_,
30 October 1987, Volume 238, Number 4827, there is an interesting

discussion of the potential effects that computers had. The most interesting parts were:

> "Large scale, distributed computing systems have been proposed in a wide variety of applications ... The automated stock market may thus hold some important lessons for the future. Indeed, recent ... research suggests that large distributed systems of this kind may be governed by ... chaos --- which means that they may be inherently unpredictable ..."
> NYSE chairman Phelan warned that "... computerized trading practices in general are a stabilizing influence only when the market itself is relatively quiet. When things become unsettled, computerized trading could all too easily become destabilizing."
> The article goes on to quote Bernardo Huberman and Tad Hogg at Xerox PARC, and their work on modeling "computational ecologies".

and...

> "The momentum for further computerization on Wall Street is clearly high. ... This momentum is leading Wall Street to delegate more and more of its day-to-day decision making power to the computers --- a prospect that many people find troubling. Of course, a hypercomputerized Wall Street might not be so different from the Wall Street of today. Brokers are already making $100 million decisions on 60-second time scales, using nothing for input but the flow of numbers on a computer screen. It is hard to imagine that they are giving those decisions any deep thought, of bringing any considered judgement to bear. What the prospect does do, however, is to throw a spotlight on the kind of economic models being used to program these computers. The economic assumptions may be valid enough for normal times."
> John L. King (UC Irvine) says "But it's like a nuclear power plant -- the emergency system is very important, even if you use it only once a year." and "what Monday illustrates to me is just how little we know."

These points make me worry more about the problems of software engineers who write software without knowing the problem domain. And furthermore, even if we/they know the domain, it may be controlled by "chaos", and may be inherently unpredictable.

Bjorn N. Freeman-Benson

Programmed stock trading

"MICHAEL R. WADE (GIPSY MANAGER)" <WADE%vtcs1.cs.vt.edu@RELAY.CS.NET> Thu, 5 Nov 87 16:28 EST

In RISKS-5.49 Bob Berger writes :

> I hope that the experience of a large network of computers doing something
> unplanned for such as accelerating the crash of the stock market will make
> the "Decision Makers" stand up and take notice! [...]

It appears that Bob has missed the "REAL" risk of this situation. The automatic trading programs all behaved as expected and correctly within their own environment. The problem is that none of these systems had knowledge, or at least only severly limited knowledge, about their external environment. The In this case we were dealing with the interaction of many independent systems where these relationships were not fully understand and/or planned for. The real risk is when system designers do not understand the relationship between all of the various components that are part of a real world environment. This has a direct impact on software certification procedures for any system, because it is not acceptable to certify the functionality of each piece of a system and then declare the system correct.

Michael R. Wade, Spatial Data Analysis Lab, Virginia Tech

Tape label mismatch (RISKS-5.55)

Jeff Woolsey <woolsey@nsc.NSC.COM>
Fri, 6 Nov 87 10:50:38 PST

In RISKS 5.55 Geoff Lane writes about an operator overriding a check for tape label mismatch causing his tape to be overwritten.

A similar thing happened to me when I was working with tapes on a CDC Cyber. The installation handled transient tapes in much the same way, except that there is no opportunity for operator intervention on a label miscompare. There is, however, nothing preventing two or more tapes being in the transient library with the same VSN (but different IDs). Furthermore, there is nothing in the operating system preventing two labelled tapes being mounted at the same time with identical VSNs, and the system will assign the one on the lower-numbered drive to the first job that wants it, even if it wanted the other tape, and even if it specified the ID. If the tape is ANSI-labelled, the system does not ask the operator for the ID written on the paper label.

In my case, I ran a three-tape archive for a friend, and when later I tried to retrieve something from the first (identical) tape, the tape was blank but had the right label. In this case it looked like the tape was re-initialized by someone else who thought they were putting labels on their own tape. Again, nothing prevents a user from entering a tape into the transient library and re- initializing it with a different VSN, possibly one of another tape already in the library, creating another opportunity for mounting the wrong tape.

On an even less-related note, I once noticed on a 4.2bsd system that the root file system was 105% full. The cause was a plain file of two megabytes called /dev/nmrt0. Some poor user thought his thesis work was on the tape he was carrying across country....

LERMINATING PREVIOUS SESSION. PQEASE RETRY.

[(Sic!) I could not resist leaving that line in. PGN]

Phantom Traffic Tickets

<portal!cup.portal!Isaac_K_Rabinovitch@Sun.COM>
Fri Nov 6 17:02:48 1987

Before David Honig concludes that he can safely forget about those phantom UCI parking tickets, he should probably read Gordon Dickson's classic SF story, "Computers Don't Argue". In this story, a book club member who doesn't want to pay for an unordered copy of "Kidnapped," by Robert Louis Stevenson is arrested for kidnapping R. L. Stevenson (a capital offense, since the victim is dead). This story might have had a happy ending, except, well, computers don't argue.

Actually, it might be irresponsible of me to make a joke of this or treat it as Science Fiction. It's worth noting that this phantom warrant might lie around various disk drives for a long time, and any traffic cop who stops Mr. Honig for a broken taillight has no way knowing that the positive warrant check is the result of a software error. While not that serious an offense, unpaid tickets *are* cause for immediate arrest -- and bail bondsmen are not anxious to cover legal amnesiacs.

Isaac Rabinovitch

National ID Card (Australia)

Tom Nemeth <munnari!augean.oz.au!tnemeth@uunet.uu.net>
5 Nov 87 00:01:32 GMT

You may be aware that recently a national ID card scheme in Australia was defeated (unfortunately only on a technicality). However, as a result, the Senate Standing Committee on Constitutional Affairs is holding an inquiry into the whole mess. Written submissions close on December 11, public hearings will begin next February, and the report is required by May. Submissions are invited from all and sundry. I enclose the terms of reference for your interest.

- = - = - = - = - = - = - = - = - = - = - = - = - = - = - = - = - = - = - = -
TERMS OF REFERENCE

(a) the provisions of the Australia Card Bill 1986 considered in the light of the reports of the Joint Select Committee on the Australia Card and of the Scrutiny of Bills Committee;

(b) the feasibility of any proposed national identity system operating in the event of a failure of any one or more States to co-operate on the establishment of a births, deaths and marriages register;

(c) the extent to which new or updated computer systems and recent crackdown campaigns on welfare cheating and tax avoidance and evasion have

obviated the need for a national identity system;

(d) the appropriate responses which should be made to the recommendations contained in the various Australian Federal Police reports on fraud against the Commonwealth and the Report of the Review of Systems for Dealing with Fraud of the Commonwealth;

(e) the direct cost to the private sector in establishing and maintaining any such system;

(f) the capacity of the proposed Data Protection Agency to adequately safeguard and protect the privacy of the individual and to control unauthorized use of any proposed national identity card and/or individual identification numbers by commercial organizations such as credit insurance companies and unincorporated associations and clubs;

(g) the desirability, timing and nature of comprehensive privacy legislation in Australia in the light of concerns raised in the debate over the proposed Australia Card legislation;

(h) the extent to which any proposed system should accord with OECD guidelines on the Protection of Privacy and Transborder Flows of Personal Data (1981);

(i) the extent of personal data held on Australian citizens by Government Departments and Agencies and by private sector agencies, its level of accuracy, access to it and its cross-referencing within the Government sector;

(j) the security of data already held by Government Departments and Agencies;

(k) the physical security of dedicated land lines and other data transmission facilities currently in use or proposed;

(l) the appropriate range and level of penalties on individuals and other entities, which should be imposed for the improper use or release of personal data;

(m) the evidence available from overseas as to the experience of other countries with identity card systems, including the taking of evidence from overseas expert witnesses;

(n) the usefulness of any card and numbering system in achieving the objectives of reducing the extent of the cash economy, organized crime and large-scale tax evasion and welfare fraud; and

(o) any matters relevant to the preceding.

(Journals of the Senate, No. 12, dated 8 October 1987)

Unix 8-character password truncation and human interface

Geoffrey Cooper <imagen!geof@decwrl.dec.com>
Fri, 6 Nov 87 14:13:06 PST

This message is quite a bit late -- I got busy, and then waited until I had time to catch up on Risks before answering.

My sincere apologies to the moderator for starting the recent barrage of Unixalia. My original comment, which has perhaps receded into the umbrageous recollections of RISKS Digests past, concerned the SILENT truncation of a password to 8 characters on 4.3 BSD. I am overwhelmed at the quantity and depth of discussion on the security of the modified DES algorithm, the propensity of a Cray to zap Sun 3 passwords with a laser, etc., all of which misses the original point (but is perhaps interesting in its own right).

The PROBLEM is that a program to set passwords sets the password to something other than its input, without warning the user. The RISK is that the user might end up with a non-secure password as a result. I have seen the same problem, exhibited by the (Massachusetts based) BayBanks automated teller system. In that case it resulted in dollar loss and a squabble between the bank and an innocent customer, when an ATM card thief was easily able to guess a password (this occured some time ago - one imagines that the problem has since been fixed). In my case, the problem resulted in an account in an obscure corner of the DoD internet that had a password which was easy to guess. The password remained for a week or two, and I don't believe that the account was penetrated (other than by me!).

We engineers have a tendency to allow our fascination with technical solutions to distract us from the issue at hand: this is a true "risk." The technical solution to the bug I mentioned is trivial -- modify the program that sets passwords to warn you when a password is being truncated. Other interesting technical solutions have been presented in this forum.

I echo PGN's recent comment that it is a poor user interface to a system's security features that is often the easiest entry point to the penetrator, rather than a deficiency in the system's operation.

- Geof Cooper

---

setuid (once more)

George Kaplan <gckaplan%sag4.ssl.Berkeley.EDU@jade.berkeley.edu>
Fri, 6 Nov 87 09:43:42 PST

In RISKS-FORUM Digest Vol 5, Issue 55, Stephen Russell discusses a bug in a student assignment submission system:

> ... It then invokes the second program, which is basically
> a setuid root file copy program. It needs to be setuid root, as it writes
> into a protected directory. The copy program is publicly executable, although
> (we believed) reasonably well hidden.

The directory has to be protected, of course, and the copy program has to be setuid, but why to root? If the assignment directory is owned by a normal user account, perhaps an account set up specifically for the class or professor, then it is just as protected from casual snooping as a directory owned by root. Then even if the security checks of the file copy program are breached, the intruder can damage only files associated with the class. This is bad news for the class, I suppose, but the system is protected.

George Kaplan Internet: gckaplan@sag2.ssl.berkeley.edu
UUCP: ...!ucbvax!ucbssl!sag2!gckaplan

Re: Minuteman Missiles (Unsung Heroes)

Mike Bell <mcvax!camcon!mb@uunet.UU.NET>
5 Nov 87 16:58:12 GMT

in RISKS 5.52 John J. McMahon says:

> ... Their immediate reaction was to take a large armored personel carrier
> (APC) and park it on the missile silo...

I'm very much impressed by this cool, clear, lateral thinking.

(Or was this the solution in the Minuteman manual?)

Surely there must be other examples of people averting `computer' disasters by unobvious mechanical means...

Mike Bell UUCP: ...seismo!mcvax!ukc!camcon!mb Phone: +44 223 358855

Mailing List Humor

Bjorn Freeman-Benson <bnfb@june.cs.washington.edu>
Mon, 09 Nov 87 15:34:12 PST

Today I received a computer-generated junk letter that had three view-through boxes in the envelope:

```
+-----------------------------------------------------+
|          Recepient            |
| If your name appears in the box below, you have won! |
+-----------------------------------------------------+
+------------------+ +---------------------------------+
|    John Brink    | | Benson            |
|    Recipient     | | ....              |
| Anne B. Meechan  | | Seattle, WA 98115         |
| Cindy Lenorowitz | +---------------------------------+
+------------------+
```

And it said inside "The names herein have been computer selected from amoung

thousands without regard to gender or affiliation." Yeah, no kidding! And without regard to their existence, too!

Bjorn N. Freeman-Benson

A new kind of computer crash

Steve Skabrat <umn-cs!rosevax!herman!sps@RUTGERS.EDU>
9 Nov 87 19:49:13 GMT

I read the following in the Minneapolis Tribune, Monday, 9 Nov 1987:

> Portable Computer Falls Out of Airlink Jet Oshkosh, WI (Associated Press)
>
> Usually a computer "crash" is caused by a malfunction in the machine. But when Ron Olstad's computer crashed last week, it really crashed.
>
> Olstad arrived in Oshkosh on a Northwest Airlink flight from Minneapolis about 3 p.m. Thursday and noticed that his portable computer was not among the luggage unloaded from the plane.
>
> At about the same time, Ronald Miller's neighbors found Olstad's 50-pound computer - or what was left of it - in Miller's back yard in Oshkosh.
>
> Robert Schoenfelder, Oshkosh manager for Northwest Airlink, said Saturday night that the port door of the airplane was open during the flight and that the computer fell out as the plane was making its final approach to Wittman Field.
>
> Schoenfelder said it is the first time that he knows of that a piece of luggage has fallen out of a plane of Northwest Airlink, which is a contract carrier for Northwest Airlines. He said Northwest Airlink replaced Olstad's computer.
>
> Miller's neighbors say they weren't startled when they heard a loud crash and saw papers flying around Miller's back yard.
>
> Two nearby elementary schools were letting out at the time and the neighbors thought it was just noisy students. It turned out to be Olstad's computer.
>
> "I noticed a branch had fallen and there were papers flying all over the back yard," said Adeline Heyer. "I didn't hear anything, but after looking a little closer I noticed the case."
>
> Miller had been gone and learned of the incident Friday.
>
> "There were papers scattered in the back yard and this big green thing," he said. The computer, which was in a canvas case, was destroyed.

My first reaction upon reading this was to laugh. My second was to wonder if any parents in the neighborhood thought they should have prepared their children to live in the area surrounding an airport by issuing them crash helmets.

Search RISKS using swish-e

Report problems with the web pages to the maintainer

Search RISKS using swish-e

THE RISKS DIGEST

Forum on Risks to the Public in Computers and Related Systems

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

Volume 5: Issue 57

Thursday, 12 November 1987

Contents

Mobile Radio Interference With Vehicles

Steve Conklin <b14!steve@uunet.uu.net>
11 Nov 87 08:47:55 CST (Wed)

My father installed his two meter rig on his new G.M. car three years ago, and every time he would key it to transmit, the engine would die. The engine control computer was rendered useless by the radio frequency field.

The reason that the car manufacturers do nothing to fix this is that they have no incentive to do so. The only laws applicable to this situation are the ones concerning how much rf energy gets OUT of the computer in the car. (A related note - this is why when the first P.C.s came out, if you called Big Blue and said that when you turned on your TV/dryer/etc you got garbage characters on the screen, they wouldn't help you, but if you said that every time you turned the system on your neighbor's TV went crazy, they would replace your keyboard, motherboard, and chassis.)

My father never found a solution to the problem. Maybe as cellular phones gain in popularity, the auto manufacturers will have an incentive to take steps to prevent rf from affecting their computer systems. This also will become a very important issue when functions other than engine control are taken by the computer.

One final issue is that of outside intentional interference. After this happened, my father and I speculated that cars with computer engine control could be disabled from another vehicle by the application of the appropriate frequency of rf energy with a directional antenna. This could be used by law enforcement agencies, or by terrorists wishing to kidnap someone, etc.

Steve Conklin, Intergraph Corp., Huntsville, AL 35807, (205) 772-6888
{uunet,ihnp4}!ingr!tesla!steve

Mobile Radio Interference With Vehicles

Bill Gunshannon <bill@trotter.usma.edu>
12 Nov 87 15:14:48 GMT

As a curious aside to Leo Schwab's article:

A letter was published in an amateur radio oriented magazine called QST a few years back by a ham who tried to install a UHF mobile radio in his newly purchased Japanese import. He too had problems with interference to the electronic ignition in the car. A call to the US Service Representative for the cars manufacturer resulted in a very simple solution to the problem. They told him "don't install the radio in the car".

A novel approach to preventing interference.

bill gunshannon

Optimizing for cost savings, not safety (Re: RISKS-5.56)

John McLeod <jm7@pyr.gatech.edu>
Wed, 11 Nov 87 02:12:56 EST

A brief comment about the cost of items in automobiles. Anything that costs a nickel more per car, and does not affect performance under normal conditions is very likely not to get done, as this will save $50,000 per million cars. The shielding of electronic ignitions and engine performance computers will cost more than a nickel per car, and does not affect performance most of the

time.

John McLeod VII, Georgia Insitute of Technology, Atlanta Georgia, 30332
uucp: ...!{akgua,allegra,amd,hplabs,ihnp4,seismo,ut-ngp}!gatech!gitpyr!jm7

"Welcome To My World", BBC1 Sundays 11PM -- A Short and General Review

<mcvax!minster.york.ac.uk!MartinSm@uunet.UU.NET>
11 Nov 1987 19:43:33 GMT

The BBC is currently showing a series called "Welcome To My World" which deals with the future of information technology. It covers areas which seem to be relevent to readers of this newsgroup so here is some information on it.

It portrays a world, not too far in the future though the exact date is not given, where development of technology has taken place without proper thought and control. Civil liberties are virtually nonexistent. A camera on every street corner watches for crime, dissent or deviation from the "norm". Computers direct almost every aspect of industry, commerce and war. Books are curious collectors items, though knowledge is more widely available - if you can pay for it.

The programme is introduced as a fictional documentary, interviews with real and imaginary people are intercut with news footage of fictional events and it presents a very pessimistic view of what life may be like. I have yet to decide whether this is because they sincerely believe it or because it makes more interesting TV. The presenter, Robert Powell, likes to say that his world doesn't have to be ours, if we make the right choices.

Extra topicality was gained a fortnight ago when one of the programmes, made months earlier, considered the possibility of a worldwide stock market crash caused by the global computer networks doing the dealing. Impressive pictures of rooms full of cabinets were shown with the implication that there is something intrinsically frightening in having computers handle money. What frightens me is the way people handle it.

Another programme dealt with databases and secrecy. In this one a fictional organisation called FREDI (freedom of digital information) hacked a top secret database and released the contents to a public network. Added spice was added by official denials that the database existed. An interesting scene showed the presenter being stopped on the street and made to state his ID number which was then checked on a terminal.

Last week a somewhat more unusual topic was chosen and interesting questions were raised. Would artificial intelligence make artists redundant? If a computer produces a work of art who owns it? Should a film director be allowed to electronically recreate actors to get certain scenes how he wants?

In conclusion then I do not think that much in this series would be new to readers of this newsgroup but it is being shown on BBC1 with a potential audience of millions. It does go out at 11PM on Sundays but I can't be the only viewer! Even though I do not agree with the viewpoint of

this programme I regard it as one of the more thought provoking things
to hit the small screen recently.

Martin Smith

Langwith College, University Of York, Heslington, York YO1 5DD England.

Re: A simple application of Murphy's Law (Tape Labels)

<decvax!utzoo!henry@ucbvax.Berkeley.EDU>
Tue, 10 Nov 87 00:26:42 est

> ...When
> you attempt to overwrite a labeled tape on our system an operator message
> appears asking if you really want to write to the tape. The operator must
> have answered yes to this question...
> This is of course an example of the seeing, hearing, reading what you expect
> to see, hear or read rather than what is actually there. There appears to be
> nothing that you can do to prevent this kind of error...

Actually, no, there are things that can be done to prevent this kind of error. I don't think you have diagnosed it quite correctly. I strongly suspect that the operator saw the question and understood it, but that he/she sees that question a dozen times a day, and the normal answer has become a reflex. *That* behavior is fully predictable and a conscientious interface designer will avoid such situations. "Do you really want to do this?" is a question that should never be asked unless there is truly a good chance that the answer will be "no".

Note also that the question was directed to the wrong person: the operator, who probably doesn't know enough about the work to judge whether the request is a reasonable one. Since the system insists on asking him/her questions that would require considerable investigation to answer intelligently, the questions will quite predictably be answered unintelligently. It is not unreasonable to request manual intervention when major data destruction is requested, but it *is* unreasonable to place the decision in the hands of someone who gets paid for throughput, not thought.

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

Overwrite of Tape Data

Ron Heiby <gatech!mcdchg!heiby@RUTGERS.EDU>
11 Nov 87 16:23:44 GMT

About ten years ago, I was doing some work where I had quite a few reels of tape (and very little disk space by today's standards). Also, I was working in an environment where I couldn't trust the operators to *not* insert write-enable rings in my tapes. I also couldn't trust them not to mount my tapes in response to a tape request from another user. The information on the tapes contained my master databases and selected subsets which were

monetarily expensive to re-derive from the masters, as I had to pay for my resource usage.

After being burned once, and losing a tape full of subsets, I ran across a tape accessory in a computer supply catalog called "write protect rings". These were thin rings of red plastic that were to be inserted into the write enable ring slot. The idea was that they would interfere with the ability to insert the write enable ring into the tape, yet would not activate the switch in the tape drive, themselves. These worked quite well for me and I had no further incidents. I took a peek at the November Inmac (major computer accessory distributer) catalog and did not find these rings. Now, I can't recall from whom I purchased them.

These "write protect" rings still wouldn't stop an operator who was determined to put a write ring in, as they were removable (with a screwdriver or an overpriced "removal tool" sold by the same company). However, the operator would have to go to some fairly extreme lengths. That, coupled with a label threatening the loss of certain body parts if a write ring were inserted in the tape would probably deter just about anybody. A similar approach could be used with the newer tape cartridges. I'm currently using 3M DC600A cartridges, and they have a rotatable write protect "notch". A sticky red label could be placed over the turning slot to help provide cues that it would be a big mistake to write on the tape.

Ron Heiby, heiby@mcdchg.UUCP Moderator: comp.newprod & comp.unix

---

Misplaced trust [Banned AIDS?]

<BSnow@DOCKMASTER.ARPA>
Wed, 11 Nov 87 12:54 EST

An entertaining quote from the Washington Post of November 10, 1987. It is from a front page story on Idaho's drive to stop AIDS.

> "Doctors, hospitals, and laboratories would be legally required to report the name and address of anyone who tests positive, information that would be kept in a locked file and on COMPUTER." (emphasis added)

Bar Codes

Elizabeth D. Zwicky <zwicky@ptero.cis.ohio-state.edu>
10 Nov 87 04:51:57 GMT

>Bruce N. Baker <bnbaker@kl.sri.com>
> The bar codes are identical ...

When you were comparing bar codes, did you actually compare bars, or only the numbers across the bottom? UPC *does* encode more numbers than the ones shown on the bottom; usually two digits, used for check digits. This is because in UPC there are four ways to encode a digit, left or right, and odd or even; the left and right ones are used to tell you whether you read the

barcode forwards or backwards, but the odd/even distinction gives a meta-code. That is, every time you read a character you have four facts about it: 1) what number it was 2) whether it was right or left 3) whether it was odd or even. The pattern of odds and evens can encode a digit. I suppose that if you knew in advance what orientation the barcode would come by in you could probably use the pattern of rights and lefts to encode another digit.

To the best of my knowledge, this feature is not used by actual UPC (that is, in the Uniform Price Code standard), but is used in EAN, the European standard which uses the same bar codes. If they use the check digits for something else, then only they will be able to figure out what they are; anything that reads UPC will reject it, since UPC specifies what the odd/evens must be, anything that reads EAN will reject it because the check digits are wrong, and programs that read both will read everything but the numbers of interest, because they ignore odd vs. even.

Of course, they could be doing something even simpler, like printing a number that is not the number encoded in the barcode above. This would probably be easier to see with the naked eye, though.

Elizabeth Zwicky,
The Ohio State University Dept of Computer and Information Science

---

Password truncation and human interfaces

Theodore Ts'o <tytso@ATHENA.MIT.EDU>
Tue, 10 Nov 87 00:28:59 EST

There is a similar problem with the (Massachusetts) BayBanks teller system: it truncates your PIN to FOUR numbers (even though they tell you to pick a PIN between four and six numbers). Yes, it's still there. When (or if) they will ever fix it is unknown.

- Ted

Re: UNIX setuid nasty -- Watch your pathnames

<munnari!elecvax.oz.au!geoffw@uunet.UU.NET>
Thu, 12 Nov 87 17:01:26 EST

Sydney Uni's fate might be seen as an example of the risk taken when an originally distributed function is centralised.
In the original give system developed at UNSW, each class instals a copy of the give/take pair. The second of these is setuid to the class account and constructs the destination pathname from entirely validated components: the class directory, assignment name and login name. The former are compiled into the program while the last is extracted from the password file.
The purpose of give is to collect the student submission only.

Now the modifications made at SU removed the responsibility for

determining the target from the relative safety of take
to the total insecurity of give, while at the same time increasing
the destructive power of take. No wonder they got into trouble.

UNIX setuid stupidity

David Phillip Oster <oster%dewey.soe.Berkeley.EDU@Berkeley.EDU>
6 Nov 87 20:08:36 GMT

munnari!basser.cs.su.oz.au!steve@uunet.UU.NET (Stephen Russell)
describes a problem that happened to him as a result of a fundametal
misunderstanding he has about the way the Unix security system
works. His misunderstanding is so fundamental that he completely
misanalyzed his problem and the moral that should be drawn from it.

He describes a task: He needed a program that would copy a file owned
by a student into a directory owned by a teacher.

The correct solution is: If the file has read access to all, then the
teacher, himself, could copy the file to his directory. Unix has a
mechanism called setuid (it stands for "set user id") that lets a user
authorize a program to act as the user's agent. The teacher can write a
program to act as teacher's agent. The student can run it, and the file
gets copied.

Mr. Russell made two mistakes.
1.) He made his program setuid "root" instead of setuid teacher. As
a result, the program let students copy into any place, not just those
places that the teacher was allowed to. This means that the damage caused
by his second mistake was not contained by the Unix protection system.

2.) When you make a program "setuid" you are giving the program the
ability to act in your name. That means that the program must check, just
as you would, that it is performing a legal act. Mr. Russell kindly explained
that he got this part wrong.

Now, all of the above works only if the teacher can read the student's
file. We need some way of arranging for the teacher to be able to read
it but not the other students. Unix also has a mechanism for doing
this. A "group" on unix is a list of users. Each file has both a user
id and a group id, and both user and group permissions. It is quite
reasonable to have a separate group for each student<->teacher pair.
If a student wants to give a copy of a file to a teacher, he runs a
program that:
1.) changes the group of the file to the student<->teacher group,
2.) runs a setuid="teacher" program to copy the file to the teacher's
directory.
3.) changes the group of the file back.

Now, if you have M students and N teachers, this means you need M*N groups.
Groups in turn are defined in a sequentially read text file, owned by root.
One can argue that having all these predefined groups would make the system

slow, but you can use a small, simple setuid=root program to dynamically create a group with just the membership it needs, use it long enough to do the copy, then destroy the group again.

The whole thing could almost be packaged as a standard utility for user A to give copies of his files to user B. User A would run such a program to give a file to user B. It would or would not do the copy based on its execution of a set of rules, written by user B, defining the circumstances that must be true for B to accept A's file. (For example: "must be smaller than 100k, must leave at least 1Meg free space on disk, must not clobber any file already owned by B.") The problem with such a packaged utility is coming up with a reasonable language for user B to express under what conditions he would be willing to recieve files.

Now, why do I need to say this? Why wasn't this all obvious to Mr. Russell? All of this is implied by the standard Unix manuals. Perhaps there should be some test you must pass before they let you have the root password.

--- David Phillip Oster --A Sun 3/60 makes a poor Macintosh II.
Arpa: oster@dewey.soe.berkeley.edu --A Macintosh II makes a poor Sun 3/60.
Uucp: {uwvax,decvax,ihnp4}!ucbvax!oster%dewey.soe.berkeley.edu

---

How much physical security? (Re: RISKS-5.48)

Martin Ewing <mse%Phobos.Caltech.Edu@DEImos.Caltech.Edu>
Sat, 24 Oct 87 01:59:00 PDT

In reply to Brent Chapman and PGN on the subject of Computer Center physical security:

I also recall the situation at MIT in the early 70's. The key punches and job submission area were on the second floor, while the CPUs were on the "secure" third floor. (The elevator wouldn't stop there.) This worked OK, until Vietnam-related movements escalated. (I was a minor participant.) At that point an actual guard was posted on the first floor, and you had to show ID to go beyond. Expensive, but apparently effective.

[The MIT CC was my first introduction to computer bulletin boards. There was a big newsprint pad on the wall, along with felt-tip pens with which to vent your spleen. The pads would disappear after some days and reappear later with Staff's annotations added. Good, appropriate technology.]

These days, I have some responsibility for a departmental facility (2 Vax 780s, a Convex C-1). Inside doors are never locked, and an exterior door to a loading dock is only about 6 feet away from the computer room. I don't foresee risks from political protests (astronomy being perceived as benign, I think), but there is always the deranged ex-student or -employee, not to mention old-fashioned vandals off the street.

There is some fractional risk from physical assault. The cost of significant improvements seems high. The value of the facility, including data files,

is high also. How does one rationally decide whether the risk is acceptable?

As far as I can see the absolute risk from power surges, flooding, and network breakin is greater. We have had instances of all of these.

My tentative answer is not to do anything about physical security. The Institute is insured against equipment losses. The one thing we don't do is to keep copies of valuable files stored in an independent environment. This can be done for fairly low cost, although it goes against the grain for researchers to make backups at all.

I'd appreciate comments.

Martin Ewing, Caltech Astronomy

How much physical security?

"Milton A. Colvin" <mac3n@babbage.acc.virginia.edu>
Tue, 27 Oct 87 10:21:21 EST

> In RISKS-5.45, Brent Chapman (koala!brent@lll-tis.arpa) writes:
> >Have there been any cases of terrorist or political attacks on comp centers?

At Dartmouth in 1969 the College was closed for a day of political activity. Instead of attacking the computer center, hordes of students headed for the terminals and used the computers to generate mail to Congress. Dartmouth had always made an effort to demystify computers.

I have this on hearsay. Perhaps someone who was there could comment.

How much computer room security?

<Mike_Alexander@um.cc.umich.edu>
Fri, 23 Oct 87 17:19:46 EDT

The various storyies in Risks recently about the effects of the student unrest of the 60s and 70s on computer room security remind me of an incident that occured at the University of Michigan during that period. It is somewhat amusing and might be of interest to Risks readers.

The University of Michigan was the scene of a number of student demonstrations and other activities (SDS was founded at UM, for example, and it was the site of the first teach-in), although there wasn't much physical damage or other real violence here. One of these incidents involved a small group of students who were attempting to shut down the University by seizing control of the University power plant, an effort that proved ineffective. The incident I have in mind occured during this protest.

At the time, the Computing Center was directly across the street from the power plant (which meant we had clean power, by the way). While the students were milling around outside the power plant, a few of them broke

off from the main group and headed toward the Computing Center. Since university computing centers elsewhere had been the object of some violence by then, the CC staff members who were watching this were somewhat concerned. However, it turned out that the students were just going to pick up some of their output, not to trash the Computing Center. Fortunately, that was as close as we came to real trouble at the Computing Center during that period.

> [Thesef last three contributions were backlogged, and reflect old history. Nevertheless I think terrorism and vandalism represent an important area to be aware of, so I dusted them off. PGN]

Search RISKS using swish-e

Report problems with the web pages to the maintainer

Search RISKS using swish-e

THE RISKS DIGEST

Forum on Risks to the Public in Computers and Related Systems

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

Volume 5: Issue 58

Sunday, 15 November 1987

Contents

Son of Stark

Hugh Miller <HUGH%UTORONTO.BITNET@wiscvm.wisc.edu>
Sun, 15 Nov 87 11:19:15 EST

The following appeared in this morning's edition of the *Toronto Star*, Sunday 15 November 1987. Here we go again:

> WASHINGTON (AP) - Deficient radar equipment aboard the USS Stark, and not the ship's crew, was chiefly responsible for the frigate's failure to defend itself against an Iraqi missile attack last May, the ship's captain said in his first extensive comment on the incident.

Capt. Glenn Brindel acknowledged "deficiencies in the watch" aboard the ship, but wrote, "Their actions or inactions ... are not primary causes for Stark's failure to defend against the ... attack.

"Unfortunately, the ship's radars and electronics did not function as advertised."

His assertion directly contradicts the official US Navy board of inquiry findings, released in a censored version Oct. 15.

It also raises new questions about the ability of similar frigates - at least six ships of the same type are currently deployed in the Persian Gulf - to defend themselves against such attacks.

Brindel expressed his views in a lengthy letter to the editor, printed in tomorrow's editions of the weekly newspaper Navy Times.

The board of inquiry harshly criticized Brindel and some of his top officers for failing to defend the Stark from two Exocet missiles fired from an Iraqi jet May 17.

Brindel said Stark's radar systems should have detected the Exocets.

"They did not," he wrote.

Brindel, the board of inquiry concluded, "failed to provide combat-oriented leadership, allowing Stark's anti-air warfare readiness to disintegrate to the point that his Combat Information Center team was unable to defend the ship."

Thirty-seven sailors died in the attack.

Would someone who has quick access to Navy Times be so kind as to send in extracts from Brindel's letter giving details? Specifically, will we now find out that the Phalanx was on after all, and pulled a Divad? Capt. Brindel, it appears, has been made to take a dive for a bad P-sub-k. Hope this doesn't hurt his pension.

Hugh Miller, Toronto, Ont.

Follow-up to Black Hawk Failures article

<ihnp4!ihlpm!dcn@ucbvax.Berkeley.EDU>
Sat, 14 Nov 87 17:33:16 PST

COPTERS GET SHIELD FROM DEADLY RADIO

Wahington - The Army, alarmed by new test results showing that radio waves

can shut down the vital hydraulic system of its Black Hawk helicopter, will shield the system's electronic controls from such interference, Army officials said Wednesday [November 11, 1987]. Radio waves triggered a ``complete hydraulic failure'' on a UH-60 Black Hawk by generating false electrical commands in the system, according to test results. The Army's decision comes after a series of crashes in which the helicopters nosedived into the ground. Since 1982, 22 servicemen have been killed in five Black Hawk crashes.

(From the Chicago Tribune, November 11, 1987 - dcn)
Dave Newkirk, ihnp4!ihlpm!dcn

Jamming the Chopper

Brint Cooper <abc@BRL.ARPA>
Thu, 12 Nov 87 8:28:13 EST

From wire service reports:

"The Army, alarmed by new test results showing that radio waves can shut down the vital hydraulic system of its Black Hawk helicopter, will shield the system's electronic controls from such interference, t Army officials said yesterday.

Radio waves triggered a "complete hydraulic failure" on a UH-60 Black Hawk by generating false electrical commands in the system, according to the Army's latest test results. When that happens, the pilot can't control the aircraft.

The Army's decision, disclosed at a private meeting this week with officials from Sikorsky Aircraft Co., the Black Hawk contractor, comes after a series of crashes in which the helicopters nose-dived into the ground.

The Black Hawk's logic module...will be replaced with the shielded version already used aboard the Navy Sea Hawk, a derivative of the Army chopper, according to Army officials."

Two thoughts:

1. If the Sea Hawk is a derivative of the Black Hawk, why is it that the former has the shielded control module and not the latter? Is the Navy smarter than the Army?

2. Didn't we have a discussion in RISKS of similar problems with electronic anti-skid automotive braking systems some time ago? Did it conclude anything?

_Brint

[Yes. Not really. PGN]

Computer systems hit by logic bombs

"J.D. Bonser" <jdb%watsup.waterloo.edu@RELAY.CS.NET>
Fri, 13 Nov 87 16:37:35 EST

Excerpted without permission from the front page of the
Toronto Globe and Mail, 3 November 1987.

Computer systems hit by `logic bombs'

In another case involving a Toronto company, a similar ``logic bomb''
was activated the day the employee's termination notice was
processed in the computer system. ``It wiped out the whole system,'',
said Sgt. Green, ... a specialist in computer crime.

In another case Sgt. Green worked on, a bank branch decided on the
occasion of its 10th anniversary to honor the customer who had the
most active account. It turned out to be an employee who had
accumulated $70,000 funnelling a few cents out of every account into
his own. ``He said: `Go ahead and charge me. I will tell the public
you have been doing this for years.' It was true. The bank had been
rounding off (customers') accounts and putting them into sundry
accounts.''

A man in southwestern Ontario acquired a printing press and ran off
thousands of bank deposit slips with the computerized code for his
own bank account on the bottom of each. Then he discreetly left
piles of them on counters at a number bank branches ... [and] the
deposits went into his account.

A number of employees of a Toronto-area machinery supplier extracted
computer lists of clients and blueprints in order to set up their
own rival company. The scheme was discovered at the last minute and
a trial is scheduled to be held soon.

Sgt. Green said current legislation is adequate to deal with the
problem. ``Our concern is people are reluctant to bring (information)
to us.''

Risk of more computers

Arthur David Olson <elsie!ado.UUCP@SEISMO.ARPA>
Sat, 14 Nov 87 14:06:27 EST

The November 11, 1987 Washington Post includes a UPI account of
President Reagan's proposed legislation on child pornography.
The proposal ". . .would give prosecutors the right to move against computer
networks and parents who permit their children to be used in pornography."

This newly discovered capability of computer networks to have children may

explain the volume of mail that's been overwhelming the moderator of late. Had the computing community known earlier what the result of connecting CSNET, BITNET, USENET, and friends would be. . .

--ado

Reach out and (t)ouch!

<Matthew_Kruk%UBC.MAILNET@MIT-Multics.ARPA>
Fri, 13 Nov 87 20:10:18 PST

Source: Deutsche Presse-Agentur

BONN, West Germany - An elderly West German woman who failed to replace her telephone receiver properly after a five-minute call to a relative in Nairobi, Kenya, received a whopping telephone bill for $2,3000.

Because of a fault in the Kenya exchange, the connection was not cut and since German telephone exchanges and billing are all computerized, the live line went unnoticed. The meter ran 10 hours.

The 86-year-old woman asked the West German Telephone Agency to excuse the debt, but the agency offered to deduct one third of the bill.

She then petitioned Parliament, which ruled this week that she would have to pay one-third of the bill for carelessness.

Re: Password truncation and human interfaces

Mark W. Eichin <eichin@ATHENA.MIT.EDU>
Fri, 13 Nov 87 15:05:27 EST

What is especially interesting (in the BayBanks case) is that
1) It is only on DieBold machines (cross-network stuff needs the whole string)
2) The screens actually flicker visibly once you have pressed the fourth digit, making this feature easy to suspect...

Mark

Mobile Radio Interference With Vehicles (RISKS-5.57)

Ian G Batten <BattenIG@CS.BHAM.AC.UK>
Fri, 13 Nov 87 12:43:43 GMT

There was some trouble a year or so ago I read of in one of the Car magazines with engine management systems on several makes of car. It appeared that when driving near Daventry (about 25 miles south of here on the road to London) their engines would die. This was traced to RFI from the powerful transmitter field there (Nationwide Radio Four, on

1500 metres is transmitted from there, along with the local Medium Wave and FM stuff. The level of transmissions around there certainly taxes my car's radio!)

ian

Computer terrorism

Brint Cooper <abc@BRL.ARPA>
Fri, 13 Nov 87 16:57:38 EST

Article 114 of comp.society:
Path: brl-adm!umd5!mimsy!oddjob!hao!ames!sdcsvax!ucsdhub!hp-sdd!hplabs!hplabsz!taylor
From: rhorn@infinet.UUCP (Rob Horn)
Subject: Computer usage by Solidarity in Poland
Date: 10 Nov 87 19:31:54 GMT

This is a sketch of the article, ``Of Systems, Solidarity, and Struggle'' in Datamation, 1 November 1987.

``You know why there are so few sophisticated computer terrorists in the United States? Because your hackers have so much mobility into the establishment. Here, there is no such mobility. If you have the slightest bit of intellectual integrity you cannot support the government.... That's why the best computer minds belong to the opposition.'' - Anonymous

This opens a good article on how computers are being used by the opposition in Poland. Go find a copy of Datamation and read it.

Solidarity is now becoming computerized. Computers are used to write articles, track election fraud, maintain organizations, and maintain communications. Using computers for such illegal purposes is not without penalties. Typical sentences for opposition activities are 1-2 years when the crimes are non-violent.

The government has focused its efforts on severing the communications that make opposition efforts effective. When they initially severed the public telephone system, computer operators used internal private line systems to maintain communications. With martial law, these too were shut down. Now the primary modes of communication are either by mail or by courier. A floppy disk is easy to hide in a package or carry unobtrusively.

Personal computers are now widespread in Poland, acquired both legally and by smuggling. There are an estimated 500,000 personal computers in Poland, with Sinclair and Amstrad being the most popular. There are an estimated 700 illegal publications being generated by everything from matrix printers to laserwriters. Nearly two thirds of the non-violent crime in Poland is associated with illegal press and opposition

activities.

The government has had to choose between the serious economic damage that would result from eliminating computers and their elimination as an opposition tool. So far, they have been forced to allow the continued use of computers.

The security capabilities of computers are also important to Solidarity. Telephone calls can be traced and monitored; floppy disks are easy to smuggle around. Paper is very bulky, hard to conceal, and hard to destroy. Floppies are very compact, easy to hide, easy to encrypt, and easy to destroy.

``Every Solidarity center had piles and piles of paper .... everyone was eating paper and a policeman was at the door. Now all you have to do is bend a disk.''

Rob Horn

Search RISKS using swish-e

Report problems with the web pages to the maintainer

Search RISKS using swish-e

THE RISKS DIGEST

Forum on Risks to the Public in Computers and Related Systems

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

Volume 5: Issue 59

Monday, 16 November 1987

Contents

Risks in Voice Mail

Peter G. Neumann <Neumann@KL.SRI.COM>
Mon 16 Nov 87 21:45:56-PST

Computerized voice mail is providing rich opportunities for creative misuse, including the exchange of all sorts of illicit information -- credit card numbers, passwords, etc. There is the old tradeoff between easy-to-use short passwords and hard-to-break long passwords. Opting for user friendliness often results in breakability. There is the problem of tracing illegal activities back to the misusers, which appears to be more difficult in voice mail than in the EMAIL counterparts, especially in that voice

mailboxes are currently harder for law enforcement agencies to identify. Something like $12 can rent you one for a month. Many familiar problems also exist, such as authentication, integrity of the messages, presence of Trojan horses (e.g., monitoring interesting calls, editing calls), etc. Ain't technology wonderful?

[For Bay Area folks, there was a nice front-page article on the subject by John Markoff in the Sunday Examiner and Chronicle, 15 November 1987.]

Stark Reality (Re: RISKS-5.58)

"LT Scott A. Norton, USN" <4526P%NAVPGS.BITNET@wiscvm.wisc.edu>
Mon, 16 Nov 87 16:43:14 PST

I sent a more detailed response direct to Hugh Miller, but here is the gist of Capt Brindel's letter to Navy Times. The failure of Stark to defend against the Iraqi Exocets was, according the Capt Brindel, due to the failure of Stark's search radars and EW system to perform as advertised. He asserts that his equipment operators, watch officers, and maintenance techs did their jobs correctly, but the equipment did not do what the FFG-7 Class Combat Systems Doctrine said it could.

To address Mr. Miller's question about the Phalanx gun, Capt Brindel said that it was not activated: "The TAO stated that had he received proper indications from either the radars or SLQ-32

Re: How much physical security? (Re: RISKS-5.48)

Rich <RMRichardson.PA@Xerox.COM>
16 Nov 87 15:51:46 PST (Monday)

> There is some fractional risk from physical assault. The cost of
> significant improvements seems high. The value of the facility,
> including data files, is high also. How does one rationally decide
> whether the risk is acceptable?

> My tentative answer is not to do anything about physical security.
> The Institute is insured against equipment losses.

This should be taken care of by trading off between investment in security facilities and insurance costs. Is the insurance company astute enough to check your physical security and adjust the premium accordingly? (Is "competent insurance company" an oxymoron? Oh, sorry. :-)

Also check the change in probability of loss against losses not covered by insurance (does your insurance cover the cost of lost work while the equipment is being replaced?). How long will it take to get replacement equipment in, up, and running? Do you "lay off" everyone who needs the computer to do their job until you're running again? What is the cost of lost opportunities during the replacement time?

Do you lose valuable people because your "slovenly security" is a

sign of incompetence? Do you lose valuable people because your "Draconian security" is unendurable?

Some thought should expand this list of questions to help you make the decisionSomewhere in the middle of all these factors is a reasonable area to operate. You could even ask your users about this.

> The one thing we don't do is to keep copies of valuable files
> stored in an independent environment. This can be done for fairly
> low cost, although it goes against the grain for researchers to
> make backups at all.

Since you have a "mainframe" (rather than workstations), it should be much easier to backup your file systems (at least the project and user directories) to mag tape on a weekly basis and take those tapes off site.

> As far as I can see the absolute risk from power surges, flooding,
> and network breakin is greater. We have had instances of all of these.

Are any of these covered by insurance? I'd guess flooding might by and power surges and breakin are not. Power surges can be protected against by equipment and I would think would be worth at least some investment. At the very least, you might save some equipment with a latch that must be reset by hand before re-applying power after an outage. This allows you to bring the system back up in an orderly manner.

If you haven't done something about network (or telephone) breakin by now, your case may well be hopeless. :-)

Rich

Navy SH-60 Seahawk helicopters

"LT Scott A. Norton, USN" <4526P%NAVPGS.BITNET@wiscvm.wisc.edu>
Mon, 16 Nov 87 14:05:58 PST

The probable reason the Navy required heavier shielding on their version of the SH-60 is that when landing on a ship's flight deck, the aircraft passes right through the main lobe of ship's air search radar(s), about 50 ft from the antenna. The need for shielding is obvious: you stare right down the radar's feed horn as it swings around.

LT Scott A. Norton, USN, Naval Postgraduate School, Monterey, CA 93943-5018

UH-60 problems

Peter Ladkin <ladkin@kestrel.ARPA>
Mon, 16 Nov 87 17:34:46 PDT

One should note that the problems with the UH-60 are of disputed origin. Aviation Week and Space Technology, Nov 16 1987, p27 , "Army Modifies UH-60s To Cut Electromagnetic Interference in Controls": "Washington - Concern

about the vulnerability of the Sikorsky UH-60 Black Hawk helicopter to electromagnetic interference has led the Army to modify its aircraft, but the Army and Sikorsky deny that electromagnetic interference has caused any crashes of the helicopter. [.....]".

One should beware of inferring by association, because of its social consequences. A case in point is the V-tail Bonanza, a light aircraft that has been in production for almost forty years. Over the years, a number were lost in unexplained in-flight breakups, some with very experienced pilots at the controls. Beech, for good legal reasons, maintained that the airplane satisfied the requirements of certification, and did not investigate. Apparently the presumption was that if they were to conduct their own tests, this could be used as evidence that they were not completely sure of the airframe quality, in hypothetical litigation proceedings (this is my personal interpretation, as well as that of others). This is not by any means unsound reasoning. They willingly conducted extensive tests when required to do so by the FAA (which seemed in retrospect to be the obvious solution - one can wonder about the FAA's tardiness). Meanwhile, many v-tail owners died. We all suffer from the consequences of this kind of political/legal conundrum, and so one should note that the facts are disputed in the UH-60 case. None of which means that the press is wrong, of course.

peter ladkin

External risks (Re: RISKS DIGEST 5.58)

John McLeod <jm7@pyr.gatech.edu>
Mon, 16 Nov 87 16:31:47 EST

Another class of risks to computers is accidents external to the complex. A couple of years age at the University of New Mexico, several of the computers were shut down by a backhoe breaking a large water main on central. The water from the main flooded the steam tunnels while the steam pipes were hot. The temperature in the computer room reached 100F, and the humidity reached 100%. This triggered the shutdown sequence for the computers. However, the air conditioners overloaded when attempting to cool this mess to a suitable temperature. The computers were down for two weeks while new air conditioners were purchased and installed.

A few weeks ago here at Georgia Institute of Technology, we had a backhoe break the power cable and the network cables. The computer was down for about 12 hours.

JOHN MCLEOD, Georgia Insitute of Technology, Atlanta Georgia, 30332
uucp: ...!{akgua,allegra,amd,hplabs,ihnp4,seismo,ut-ngp}!gatech!gitpyr!jm7

Re: A simple application of Murphy's Law (Tape Labels)

Barry Gold <lcc.barry@SEAS.UCLA.EDU>
Sun, 15 Nov 87 10:46:13 PST

In designing the "secure" operating system KVM/370, we considered the

danger of an operator mounting the wrong tape from a different perspective. In an environment that mixes applications with different classification levels, an operator error can result in the data on a Top Secret tape becoming available to a user who is cleared only to Secret--or in Top Secret data being written on a tape whose external label claims it is "unclassified".

We decided to assign a separate "authenticator" to each removable volume (tape OR disk). The design was to work as follows:

Every volume, even "foreign" tapes, is assigned a volume id ("name" and/or location when racked) AND a "password". This information is entered in a database, along with the classification level and owner. The "password" is NOT given out, but is written on the tape's external label.

When requesting a tape mount, the user specifies the volume id. The operator retrieves the tape (or disk) and gives the system the volume id, the name of the user who is to receive access, and the "password".

The system checks that:

1. the "password" is correct for the volume id.

2. the classification level of the tape matches the user's current classification level. (A user cleared to Top Secret can choose to work on the Unclassified subset of his data, but will then not get access to Top Secret tapes!)

If either of these checks fails, the operator is prompted to try again. The operator can try again with the same tape (possible typing error) or a different one, or abort the mount request.

Note that there's no deep dark secret about the volume's "password". It's just a check that the right tape has been mounted.

I think the above scheme would also work to protect against accidental destruction of data in an unclassified environment. Just leave out the classification check.

You might or might not get additional protection by adding a check that the user who is to get access is the owner. If not, the USER gets a prompt "do you want to read (viz write on) xxxx's tape?" You could even add a third password that the user gives out to people who should be able to write on that tape.

Of course, the operator can always get around these checks by "adding" a new tape and claiming that the tape to be mounted is that tape, or by calling all tapes a certain standard one with a known volume id and password. You need to make sure that operators understand that just ONE use of that facility that results in overwriting the wrong user's tape will get them fired.

EAN and PIN codes

<MAKELA_O%FINJYU.bitnet@csl.sri.com>
Mon, 16 Nov 87 10:42 O

In RISKS 5.57 Elizabeth D. Zwicky writes:
>To the best of my knowledge, this feature is not used by actual UPC (that
>is, in the Uniform Price Code standard), but is used in EAN, the European
>standard which uses the same bar codes. If they use the check digits for
>something else, then only they will be able to figure out what they are;
>anything that reads UPC will reject it, since UPC specifies what the
>odd/evens must be, anything that reads EAN will reject it because the check
>digits are wrong, and programs that read both will read everything but the
>numbers of interest, because they ignore odd vs. even.

This is both correct and not. The EAN standards actually comprise of two distinct product coding systems: the EAN-8 and the EAN-13. The EAN-8 is an eight-digit no-frills barcode which is encoded only in the "set A" bars. The EAN-13 comprises of 13 digits (see, we aren't superstitious over here :-) coded into a dual barset of 6 digits each. The 1st digit of the product code is encoded into the usage of "set A" and "set B" bars in the first barset, and the last (13th) digit of the barcode is a checksum from the previous 12 digits. So the EAN-13 barcode looks something like this:

```
          !!!!!!!!!!!!!!!
          !!!!!!!!!!!!!!!
          !!!!!!!!!!!!!!!
         0!123456!789012!
```

With the first "0" being the digit encoded into the A/B bars in the first barset. The second barset does not contain any coded information in the usage of bars, it is done simply in "set C".
Why this type of encoding was chosen, beats me! It is however compatible with the american UPC coding, since I once tested a bar code reader program with mixed EAN-codes and UPC-extended codes (you know, the ones you get on book covers with the price on a little extra barset after the main code).

Also, in RISKS 5.57 Theodore Ts'o writes:
>There is a similar problem with the (Massachusetts) BayBanks teller system:
>it truncates your PIN to FOUR numbers (even though they tell you to pick a
>PIN between four and six numbers). Yes, it's still there. When (or if)
>they will ever fix it is unknown.
Can someone out there in netland tell me how the international PIN system works (in principle, I'm not expecting the top secret algorithm :-) ?
The cards one gets around here have a 4-digit PIN field in the magnetic stripe plus one digit of "PIN version". The PIN system would seem to me to be a *very* great risk indeed, since as far as I know, the cash registers that can take a PIN code from a keypad instead of having you sign a sales slip ARE NOT CONTROLLED ITEMS, ie. I could just go out and buy one. At least, an organized and determined group of criminals could steal one. I would assume that the part of the cash register that handles PINs works on the "black box" principle, that is you feed in a card number and what was typed on the keypad and it says yes or no. The problem is that a maximum of five digits on the PIN (if we count the "version" in) would give only 100000 possible codes. One would not

have to actually reverse-engineer this device (how about calling it a "PIN Black Box" ?), only use it for testing through the possible keys.
It's designers would have taken reverse-engineering into account (per the PIN security requirements), but an attack of this type would be very hard to counteract in the design criteria, since the actual Black Box has been obtained, and can be used at leisure for "cracking" card security.
On the other hand, a determined person with enough technical skill could most certainly reverse engineer such a device. A public knowledge of the PIN algorithms would make stolen/lost credit cards a real disaster, since most of your money would probably be gone even before you could get to a phone.
Comments, anyone ?

Otto J. Makela, U of Jyvaskyla, Kauppakatu 1 B 18 SF-40100, Jyvaskyla Finland
voice phone: +358 41 613 847 BBS phone: +358 41 211 562

Computerized Fuel Injection (RISKS DIGEST 5.58)

<James_M._Bodwin@um.cc.umich.edu>
Mon, 16 Nov 87 11:10:44 EST

In the mid seventies Volkswagen developed a fuel injection system for all of their vehicles. The system has a logic box that that measures the rate of air flow and then controls valves attached to the injectors in order to obtain the correct air/fuel mix.
According to the story I heard, the system worked fine in Europe so they brought a few models over to the US to test out. For some unexplained reason the cars would occasionally stall out completely and fail to restart. Then, a few seconds later (before thgey could even get the hood up) the engine would start working again. This delayed shipment of the cars to the US market. After much head scratching someone finally figured out the problem: CB radio transmissions from nearby cars were inducing enough current in the injector control wires to cause the injectors to malfunction. Of course, the problem went away as soon as the CB stopped transmitting or when the car got a reasonable distance away. The problem was only noticed in the US because of the relatively large numbers of CBs in this country (remember the CB craze in the 70s?). The fix was to shield the control wires.

Unfortunately, this was long enough ago that I can't remember my original source for this story nor can I verify its accuracy.

I don't know enough about the power or frequencies used by CBs and cellular phones to know whether or not they are significantly different. However, CBs remain popular enough that I'm surprised that the car companies haven't already taken sufficient steps to sheild car electronics from radio transmissions. Or perhaps they just designed them to filter out junk in the CB frequencies.

Re: Password truncation and human interfaces

Franklin Davis <fad@Think.COM>
Mon, 16 Nov 87 13:01:36 est

Mark W. Eichin <eichin@ATHENA.MIT.EDU> writes:

What is especially interesting (in the BayBanks case) is that
2) The screens actually flicker visibly once you have pressed
the fourth digit, making this feature easy to suspect...

In fact, on the newer machines I can't enter my password at my normal rate -- the system pauses after the fourth digit, and won't accept the fifth for a moment. A poor interface indeed!

--Franklin

Search RISKS using swish-e

Report problems with the web pages to the maintainer

Search RISKS using swish-e

THE RISKS DIGEST

Forum on Risks to the Public in Computers and Related Systems

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

Volume 5: Issue 60

Wednesday 18 November 1987

Contents

Swedish trains collide

RICK BLAKE (on Essex DEC-10) <rick@ESSEX.AC.UK>
Wednesday, 18-Nov-87 13:31:53-GMT

From The Times, Tuesday 17th November 1987 (reproduced without permission)

> "Gothenburg (AP) - Two Swedish express trains collided at high speed
> in a suburban station at Lerum yesterday, setting a locomotive and
> a carriage on fire and trapping some passengers in the wreckage
> for more than two hours.

> At least nine people were killed and 100 injured. Two carriages were so badly twisted that they were sealed shut. The automatic system designed to prevent trains from being on the same track had apparently been shut off while work was done."

The last sentence points up a possible Risk that has been discussed before in these columns; what happens when automated systems that are designed to prevent human error are disabled? Clearly it is too early to draw any conclusions from this incident until more facts are known, but it is quite possible that, if the system worked reliably, the train controllers may have lost familiarity with the manual procedures. Alternatively, perhaps news of the service withdrawal was not adequately disseminated. The fact remains that withdrawal of automated systems may of itself constitute a Risk.

Rick Blake, Computing Service, University of Essex, Wivenhoe Park, COLCHESTER C
+44 206 872778

Hardware and configuration control problem in a DC-9 computer

Nancy Leveson <nancy@commerce.UCI.EDU>
Tue, 17 Nov 87 06:51:08 -0800

Mike DeWalt of the FAA Certification Office in Seattle sent me a copy of the Federal Register of August 7, 1987 which contains a notice of a proposed airworthiness directive, applicable to certain McDonnell Douglas Model DC-9-81, -82, -83 series airplanes, that would require inspection and modification, if necessary, of certain Honeywell Digital Air Data Computers (DADC). It reports that "This proposal is prompted by reports of erroneous information being transmitted to the Digital Flight Guidance Computer from the DADC. This condition, if not corrected, could lead to an aircraft stall close to the ground during an automatic pilot or flight director go-around maneuver."

It goes on to explain in more detail: "During an automatic go-around maneuver on a McDonnell Douglas Model DC-9-80 series airplane demonstration flight for the FAA, a simulated engine loss resulted in an electrical transient, which caused the Honeywell P/N HG280D80 Digital Air Data Computer (DADC) to send an erroneous low value of computed air speed to the Digital Flight Guidance Computer (DFGC). The DFGC used this value as a go-around speed reference and generated a large pitch-up command when it compared the actual airspeed to the erroneous reference airspeed. The automatic go-around demonstration was terminated by the pilot when the stick shaker was activated by the stall warning system."

"Investigations by Honeywell indicated that a complementary metal oxide semiconductor random access memory chip installed on Microcomputer Circuit Card Assembly (CCA) A1 could output erroneous computed airspeed, Mach, and total pressure data, without a failure warning, in the event of a power interrupt to the DADC. Modification 8 to the DADC, which consists of the addition of a transitor to the circuitry on CCA A1, prevents this from occurring. This transistor had been previously incorporated by Honeywell as a product improvement on DADC manufactured since May 1983,

but no marking of any kind was put on the DADC to identify it as having incorporated the transister. DADC manufactured after February 1987, however, have the transistor incorporated and the modification is identified by a Modification 8 marking on the DADC."

The notice goes on to describe the directive which would require inspection and modification, if necessary, of the implicated DADC on -81, -82, and -83 series DC-9s (McDonnell Douglas started inspection and modification of the DC-9-80 series airplanes in March 1987) within 12 months of the effective date of the directive.

Ethics, Liability, and Responsibility

"Gene Spafford" <spaf@purdue.edu>
Tue, 17 Nov 87 11:06:43 EST

Sometime in the next few semesters I hope to be offering a seminar course tentatively entitled "Ethics, Liability, Responsibility and the Software Engineer." This course is intended to foster some discussion about the impact of computer technology on society (for good or bad), and explore some of the legal and ethical problems involved.

Related to that:

1) The book I've been examining for the primary text should be of interest to the readers of this forum. It contains selected essays on the role of professional ethics (including the full texts of the ACM, IEEE, and other association codes of ethics), the difficulties with litigation for computer-related problems, and the role of computers in "power" systems (economic, political, etc.). The book is:

Ethical Issues in the Use of Computers
D. G. Johnson and J. W. Snapper
1985, Wadsworth Publishing, Belmont CA
ISBN 0534-04257-0

The book is available in paperback and I definitely recommend it.

2) I would appreciate suggestions from RISKS readers for other texts, essays and articles which would be appropriate for such a seminar class. I hope to compile a reading and resource list for the class, then have students pick items to study and present to the others. If you have any suggestions for such items, I'd appreciate hearing about them; actual copies would be especially welcome. I would also welcome suggestions from anyone who has taught a similar course. You can send me your suggestions via e-mail (spaf@cs.purdue.edu) or:

Gene Spafford
Software Engineering Research Center
Dept. of Computer Sciences
Purdue University
W. Lafayette, IN 47907-2004

Anyone sending me SURFACE MAIL requesting a copy of the resource list will get a copy sometime in the next academic year when I teach the class; that may not be until January 1989, so let me know if

you want a partial list sooner.

Blackhawks and Seahawks

<mlbrown@nswc-wo.ARPA>
Mon, 16 Nov 87 16:12:38 est

In Risks 5.58, Brint Cooper writes about the EMI problems with the Blackhawk and asks why the Seahawk has a shielded control module while the Blackhawk does not. I suspect that the Seahawk's shielding is a result of the Navy's stringent testing in the areas of Electromagnetic Vulnerability and EMI. The Navy's operational environment is generally very "dirty" from the EMI standpoint with all of the high power radiators aboard the ships. It is critical that, during the crucial landing phases on a moving deck, the ship-board transmitters not interfere with the electronics. This could be accomplished by shutting down the transmitters (EMCON) but this is not acceptable from an operational standpoint. Therefore, the helo has to withstand this environment.

I rather suspect that the Army's lack of shielding is a pure and simple weight vs. benefit issue. If you can save a few pounds in the design of the system, you have more available payload capacity. Often this translates into this kind of a problem. In order to meet design (e.g. payload) require-ments, things like "unnecessary" EMI shielding are done away with. When delivered, the helo meets requirements for payload and it's only later that problems like this surface. The shielding is added, the usable payload reduced, and everyone is happy (well, almost). Conversely, we can have occurrences where the original system may have satisfactorily performed in high EMI environments but an upgraded system using computers does not. The relatively low voltage, rapid response time circuits are sensitive to the EMI whereas the high voltage, slow response analog circuits did not. This is a critical issue that has to be addressed in applications where computers are used to replace analog controls.

Mike Brown

[Also noted by "pat" and Henry Spencer.]

Mobile Radio Interference With Vehicles (Re: RISKS-5.58)

Peter Mabey <mcvax!stl.stc.co.uk!phm@uunet.UU.NET>
Wed, 18 Nov 87 10:14:10 GMT

>RISKS-LIST: RISKS-FORUM Digest Sunday, 15 November 1987 Volume 5 : Issue 58
>Subject: Mobile Radio Interference With Vehicles (RISKS-5.57)
>From: Ian G Batten <BattenIG@CS.BHAM.AC.UK>
>There was some trouble a year or so ago I read of in one of the Car
>magazines with engine management systems on several makes of car...

This reminds me that when the Home Chain of radar stations was being set up in 1939, it was rumoured that the mysterious transmitting pylons being constructed were for a secret weapon that would stop the engines of the German bombers. There were reports of car engines

unaccountably stalling and refusing to restart till a technician from an adjacent hut came out, noticed what had happened, and returned inside. This was long before electronic engine management, and I doubt that the pulsed signals would have been able to have the reported effect on a conventional ignition system, so I suspect that the reports were 'disinformation' spread to put spies on the wrong track. (You never heard the stories at first hand, it was something like ...'our milkman said it happened to a friend')

Peter Mabey (phm@stl ...!mcvax!ukc!stl!phm +44-279-29531 x3596)
Standard Technology Ltd., London Road, Harlow, Essex CM17 9NA, U.K.

VW Fastbacks/RFI/EFI (Re: RISKS-5.59)

David Lesher <hadron!netsys!wb8foz@uunet.UU.NET>
18 Nov 87 04:48:39 GMT

I remember a VW mechanic across the street from the local gas station the police frequented asking me why the pancake engine (i.e., Fastbacks+Squareback) models stalled when the police transmitted. I explained it to him. This was on 150 mhz @ 100 watts out. BTW those fuel injection controls were all discrete transistor...Nobody had heard the words IC-opamp.

CB frequencies and power

John McLeod <jm7@pyr.gatech.edu>
Wed, 18 Nov 87 15:51:06 EST

CB's run at 4 Watts. Their wavelength is 436 inches. (~11m).

JOHN MCLEOD Georgia Insitute of Technology, Atlanta Georgia, 30332
uucp: ...!{akgua,allegra,amd,hplabs,ihnp4,seismo,ut-ngp}!gatech!gitpyr!jm7

Signs of the Times [1984? and Information Vending]

<RMorris@DOCKMASTER.ARPA>
Tue, 17 Nov 87 15:17 EST

A sign on Route 95 in Delaware to be seen just after passing the toll booths for the Delaware Memorial Bridge reads "Information Police".

A sign on Route 95 in Pennsylvania just north of the Delaware border reads "Weather Info Vending Machines".

The Mercaptan goes down with the strip

Burch Seymour <sun!gould!augusta!bs@ucbvax.Berkeley.EDU>

Mon, 16 Nov 87 22:02:27 EST

[OK, this isn't really computer related, but I thought it might be interesting as it's sort of high tech related.... and I kept it short too!]

The December 1987 Discovery magazine reports that the Baltimore, Maryland utility commission sent out their "Energy News" bulletin with a special addition. To help promote public recognition they added a scratch and sniff strip that smelled of mercaptan, the chemical added to natural gas to make it smell. Natural gas is odorless; the smell is added as a safety feature so users can notice potentially explosive leaks. There was a problem. The smell penetrated the unopened envelopes, causing hundreds of customers to call the fire department to report gas leaks. "People were panicking at first. They really thought they were having problems."

The brochures were shelved.

-Burch Seymour- ...sun!gould!bseymour or something like that

Re: Reach out and (t)ouch (RISKS DIGEST 5.58)

Michael Wagner <WAGNER%DBNGMD21.BITNET@CNUCE-VM.ARPA>
17 Nov 87 18:48:34

> BONN, West Germany - An elderly West German woman ... received a
> whopping telephone bill for $2,3000.

Wie, bitte? The number actually printed in the article has some sort of problem, since people in North America don't normally write a number that way. I tried to figure out what amount this really was. $23,000 is completely out of line. If it is $2,300, I can't reconcile this with the information in the story (10 hours) and the rate schedules I have here. I'm currently trying to find out more details of this story.

[Add to that the fact that 2,3000 auf deutsch is 2.3000 auf englisch. PGN]

> The meter ran 10 hours.

To me, this points out the 'brittleness' of some of our 'high-tech' services. Older services, like electricity and water service, intrinsically limit the amount of resource which can be consumed in a short time to some 'small' multiple of the 'normal' usage. This little old woman probably calls her relatives in Nairobi once a month for 10 minutes. For those 10 hours that her phone was off the hook, she was responsible for 4000 times her normal usage. I don't think you can get 4000 times normal water flow for 10 hours out of your tap, and I don't think you could get that much electricity out of the wall without melting your entrance fuses.

I must admit that those limits are the results of physical

properties that are built into the delivery mechanism (friction in the pipes; heating of the wires and fuses in the service entrance). The telephone is somehow 'better' because it doesn't have the non-linearities that give rise to these phenomina. However, those very non-linearities often serve a useful purpose in 'turning back the curve' in situations where a fault has occured.

One hopes, for instance, that if they bring the electricity to the house of the future with superconductors, they remember to use some 'normalconductors' in the service entrance to limit the total possible consumption to reasonable limits, for safety and billing reasons.

Similarly, phone systems and computer systems should contain some reasonableness checks to detect outlying situations and alert staff to them.

> She then petitioned Parliament, which ruled this week that she
> would have to pay one-third of the bill for carelessness.

I asked a friend about this; they were surprised that she got off so lightly. It is somewhat unusual that she was 'excused' from her full liability. The telephone system is an incredibly powerful institution here in Germany (and more or less in all of Europe, I gather). They do, with alarming regularity, make billing mistakes. And, being a part of the executive branch of the government, they have the muscle to make people pay the bills, even when the bill is under dispute.

Michael

Search RISKS using swish-e

Report problems with the web pages to the maintainer

Search RISKS using swish-e

THE RISKS DIGEST

Forum on Risks to the Public in Computers and Related Systems

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

Volume 5: Issue 61

Wednesday 18 November 1987

Contents

Risks of increased CATV technology.

Allan Pratt <imagen!atari!apratt@ucbvax.Berkeley.EDU>
Mon, 16 Nov 87 13:23:05 pst

I would like to assess the risks of increased CATV technology. I refer to addressable converters. Questions below are asked both for information and to stimulate thought on this subject:

The cable company serving the community where I live is upgrading their service to new, addressable converter boxes. These boxes offer remote control and time-programmable control to the user, so you can (for instance) record programs from two different channels at different times on your VCR. (Formerly, only one channel could be programmed, because the channel selector was strictly manual.) The box even reads the time and date off the air! The box also offers parental lockout of user-selected channels. Those are the user-visible benefits.

The more insidious side of this box is that it can be individually addressed from any cable company office in the area. I assume that the box monitors a frequency band (like the vertical blank interval of the cable-information channel) and watches for a command tagged with its ID. The only commands I know of are "enable/disable channel X." The box also reads the time and date off the air (!).

What other commands are available?

How much information can the box transmit back to the host? Can it say what channel it is tuned to? (Instant ratings.) Can it report how many times it was tuned to The Playboy Channel? I don't like the idea that a person or persons unknown will have the opportunity to pass judgement on my lifestyle like that. (No, I don't really get the Playboy Channel, but Showtime has its share of skin flicks.)

The box also has a mute feature. Advertisers could interrogate this to see what commercials I was actually listening to.

The Big Picture? This technology threatens to provide instant access to advertisers and other interested parties to my television viewing habits, and can even suggest whether or not I am home. And it can do all this *remotely* and for *everybody*. Couple it with laser-scanned shopping lists and computer-verified checks, and you can match person with product with commercial-viewing. The technology already exists to target one small area with one commercial, and another with another, and compare the results.

(Of course, I could always go back to broadcast-only TV. I am not paranoid enough to do that yet. I speak of capability (present and future), not intent. Still, it does give one pause...

Opinions expressed above do not necessarily -- Allan Pratt, Atari Corp.
reflect those of Atari Corp. or anyone else. ...ames!atari!apratt

---

Bank networks

David G. Grubbs <dgg@dandelion.CI.COM>
Tue, 17 Nov 87 14:57:54 est

About four years ago I worked on the custom installation of a point-of-sale (POS) system. Point-of-Sale terminals are those little slotted boxes retailers slide your credit card through when you make a credit purchase.

The software we started with was written years before (in assembly language). Its main component was a scheduler whose job was to "switch" transactions from the bank's customers (a cadre of retailers to whom the bank sold POS services) to the credit card networks and back again with authorization numbers. Our job as installers was to write the drivers for the specific credit-company network protocols and define some routing algorithms. Timing, logging, report generation and other services were already in the base system.

I learned all sorts of interesting things about the use of credit cards from the bank's standpoint. From simple items like checksum algorithms or number assignments (VISA card numbers all start with 4, Master Card with 5, AMEX with 37, etc.) to oddities of the business, like the loud emergency alarms which go off in the card company machine rooms when the synchronous network signals failed. Thick books detailed the protocols.

I also learned something I had not known to that point: Banks are not one entity. Each bank is really a collection of competing fiefdoms, whose arena of competition is both physical and financial and whose competitors are bank Vice Presidents. Bank Vice Presidents may adequately be characterized by two of their criteria for new computer systems: 1. It must fit in an area which the responsible VP "owns" and 2. It must be as incompatible as possible with other systems currently in use within the entire bank. I considered this revelation an answer to the question of why so many small, unusual computer companies can keep making a profit. To the bank VP mentality standardization is just a way of losing control of the barony, the land and the serfs.

As part of the POS package, and since I was responsible for the credit card company protocols, I had to deal with Telecredit. Telecredit assumes the financial responsibility in cashing a customer's check, for a price.

The retailer types in your driver's license number, the issuing state, your name, and the amount of the check. A packet containing the typed data is massaged by the POS terminal driver into "standard internal" format and is sent to the Telecredit driver for transmission. The driver formats the data into a packet and ships it to Telecredit. Telecredit sends back an OK or failure, which is reformatted and displayed on the originating POS terminal. (I am simplifying. There were also error conditions and some subtle failures. A card company may return codes like "Keep the card." We were asked to filter this response, since it was originally intended for ATM's, not some poor clerk at a POS asked to take Arnold Schwarzenegger's card away from him. A friend who works with these POS terminals tells me:

> "Keep the card" is definitely meant for retail personnel, who are often instructed to retain a credit card and return it to the card company, who promptly issues a check made out in the name of the clerk (for hazardous duty :-). This happened to me a couple of times. I made $25 each time. In each case, the customer shrugged and handed me another piece of plastic.)

I tried to find out how Telecredit works, but the surliness of the Telecredit people was amazing. ("We're not about to tell you our business!") It was not difficult to envision how it works, though nothing was ever verified. An OK from Telecredit means that Telecredit will assume the financial risk in cashing the check. It is a service purchased by the bank. My guess is that unlike credit card companies, which expect transaction data to come from cards provided at your request, Telecredit maintains a large database of data collected only by interaction with the public.

Some time ago, they started with an empty database. Using statistical data collected from friendly banks (who don't usually publish such things) on the number of bad checks passed, they gamble on license numbers for which they have no track record. After the first gamble, they have a track record for that individual, positive or negative. From then on they make better and better guesses based both on individual and statistical analyses of their own database. (Which is probably more accurate than one thinks, considering that the data it collects is biased for "those who will put up with a Telecredit check".) One thing I could not determine was whether they absorbed other databases containing data supposedly indicative of financial reliability, like the standard credit references one can obtain on request.

More from my retailing friend:

> When we (at my store) were deciding whether to become a Telecredit customer, they were willing to tell us quite a lot about how they worked. Generally your guess is correct. They do work as you describe, except that what I was told is simpler than your reverse engineering. They told us that any customer was considered innocent until proven guilty once. A bad check (they covered these if they approved them; for us, it was a form of insurance) was good for 90 days on their "bad-check passer" list. They also told us they were independent of anyone else's data.

One day, I was approached by my manager (not a bank employee) and asked to look at the Telecredit transaction log, not normally part of my job. The printout was five feet tall. The manager smiled, thumbed through one stack and said, "You don't have to look hard to see what I'd like you to see." As he thumbed through the reports, labeled "Telecredit Transactions -- <date> --", the column containing the check amount twinkled slightly in the last two digits, but to the left of the decimal point, there was nothing, a blank. We kept looking.

Every transaction was for less than a dollar, all 160,000 of them. The vast majority were exactly zero. And every transaction was OK'd by Telecredit.

You'd think that something in the software at Telecredit might catch this. I thought so too, until it was explained to me that it was common for retailers to run a "$0.00" transaction simply to see if the driver's license was valid. A certain misuse of the system. An OK didn't mean the driver's license was OK, it meant Telecredit had no current negative record for the license.

Many of the transactions were for large sums, as the bank found out when the retailers deposited them. Since the "bank's" software had taken valid check amounts varying from zero to tens of thousands of dollars and had truncated the dollar figure from every transaction, it was not Telecredit's fault. I believe (though I could not verify) that the bank lost hundreds of thousands of dollars.

The reaction of the Bank officer was surreal, at least to someone like me, who uses scientific notation for anything over a thousand. They decided that it was worth more to the bank not to withdraw the service, even temporarily, than it cost them in bad authorizations. So we were ordered to fix it live.

I found the bug in the POS terminal driver. Some programmer I'd never hire had tried to make a two pass loop out of an "ascii-to-integer" function and zeroed the register within the loop. It set a register to zero, parsed the dollars, set the same register to zero and parsed the cents. The register then held binary cents. I figured out a two instruction patch to the running system and patched it live, made the corresponding change to the source, compiled and installed it so the next restart would get the new code.

I think this illustrates many different computer risks:

1. One of my favorite computer risks involves the assignment of special

human-oriented meanings to "zero" which are not fully accessible to the computer's understanding. (If you'll allow this loose usage of "understanding" as a synonym for "programming".)

In different instances, Zero may mean:

Uninitialized False Error OK Empty
End-of-Line Balanced Neutral Test Waiting
etc.

Here it meant "test", but it was also an "error".

2. Telecredit is another group collecting cross-reference data on us. Like monitoring mail systems to get "known associates" lists.

3. The bank already had POS software, at least two different versions. The policy of internal competition and the maintenance of separate fiefdoms inside the bank creates a chaotic environment which knowledgeable persons may exploit. And have.

4. "What about testing?" you may ask. We did test. We tested a lot. The software at fault was unchanged from the base system, one of the few things we took for granted, since it had been installed in at least 10 other sites across the country. The teams working on the other sites had never noticed this. I was not told why. It is possible that we were guinea pigs, or the software was sabotaged. (I know it sounds paranoid, but in that environment it was plausible. I left the consultant/contractor world from this experience, miserable in many respects.)

5. Our money is managed by people who care nothing for the details of an single transaction. They sell financial services like the grocer sells apples. So what if a few are dropped on the floor? It's just a "cost of doing business." As the throughput of transactions increases over time, each detail gets commensurately smaller. It can only get worse.

David G. Grubbs, Cognition Inc., 900 Tech Park Drive, Billerica, MA 01821
UUCP: ...!{mit-eddie,talcott,necntc}!dandelion!dgg
Internet: dgg@dandelion.ci.com (617) 667-4800

John Pershing <PERSHNG@ibm.com>
17 November 1987, 10:35:23 EST

I cannot speak for *all* ATM and POS systems, but the major banks generally know what they are doing with respect to PIN security. The PIN number is *not* stored on your ATM card -- it is stored in your bank's database and, possibly, in one or more interbank clearinghouses. This makes it possible to have your PIN changed without getting the card re-magnetized (assuming your bank has it's act together). Note that your account number probably isn't even written on the card -- only a number that identifies that particular card.

When you enter your PIN and transaction request, this data is put into a message along with a serial number, encrypted, and sent up to the computer center. The proffered PIN is checked against the one in the database, and the response to the transaction request (yea or nay) along with another serial number is encrypted and sent back to the ATM. There are systems in operation (e.g., the major interbank clearinghouses) that can consistently give near-instantaneous responses, so it may seem that PIN verification is being done locally at the ATM.

If one were to go out and buy an ATM or a Point-Of-Sale cash register, it wouldn't help much in "breaking" PINs unless you could get yourself wired into a bank's network -- something which is *quite* hard to do. Even if you could tap in, you would probably have a hard time guessing the (DES) encryption keys needed for upstream and downstream traffic without raising an alert on the network operator's console.

An aside: The length of a PIN number, as we all know, is a compromise. It needs to be short enough so that it is readily memorized, to discourage the practice of writing it down (usually on the ATM card itself!). In my meager experience, 4 digits is even too long to satisfy this constraint for the bulk of the population. Keep in mind, too, that one must have the physical "key" (the ATM card) in addition to the PIN; so it is not quite as big of an exposure as, say, a short logon password.

John A. Pershing Jr., IBM, Yorktown Heights

Re: more on computer security

<[..., at contributor's request]>
17 Nov 87 11:27:33 PST (Tue)

Some recent security developments at my site (and others) are starting to cause complaints. Where military and some civilian sites have these requirements pro forma, people have a greater feeling of doing work in the public interest. Recent fears of system crackers entering, reading privacy data, potentially modifying any data, puts the Government in an awkard position between police state and protector of public interest.

This makes working in networked environments even more interesting. A sample login session now appears as follows:

Welcome To [. . . that single word is part of the problem . . .]

[. . . this part of session removed . . .]

You are connected to a U.S. Government computer system. Any unauthorized ATTEMPT to gain access to this system may subject you to fine and/or imprisonment.

Username: [. . .this part of session removed . . .]
Password:

NOTICE: This system does not provide access control
protection sufficient for the storage, processing,
or communication of classified, highly sensitive, or
proprietary information. Protection of other sensitive
information is a USER RESPONSIBILITY.
<End-of-session>

We are just now getting complaints because of words like "imprisonment." The justification for this coming from DOJ was that: "If you have a `fence' that delimits property, don't come to us if you don't have warning signs [space as such and such a distance and such and such a size. We can't prosecute." Some of our users are using words similar to a recent net posting mentioning Draconian police states, and hence, are thinking of going to the ACLU. These warnings are currently restricted to certain types of systems, but technology changes potentially worsen the problem: networks (from which they are threatening to disconnect totally), workstations and personal computers, and so forth.

The text comes from Washington DC. Middle management does not feel it can explain all of the justification since the material comes from a document under the new Sensitive classification. They feel it was done with a bad PR job. But they also realize that Congressmen control overall spending: i.e., not responsible for Government property (computing), hence, take it away.

I am curious what other scientific sites are doing in similar ways.
Please skip the obvious (secure computers aren't on networks, or passwords or encryption). We are talking civil liberties as part of this discussion.

Search RISKS using swish-e

Report problems with the web pages to the maintainer

Search RISKS using swish-e

THE RISKS DIGEST

Forum on Risks to the Public in Computers and Related Systems

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

Volume 5: Issue 62

Friday, 20 November 1987

Contents

A Two-Digit Stock Ticker in a Three-Digit World

Chuck Weinstock <weinstoc@SEI.CMU.EDU>
Fri, 20 Nov 87 17:06:42 EST

From Business Week, November 30, 1987, Page 108I
(Industrial/Technology Edition):

When the Dow Jones industrial average plunged 508 points on Oct. 19, the message didn't get through to subscribers of Lotus Development Corp.'s Signal service, which provides up-to-the-minute market data. Because Signal can record only a two-digit net change for each day, it reduced the market crash to eight points. "When the product was originally designed, they didn't take into account these sorts of fluctuations," concedes Lotus spokesman James P. O'Donnell.

Signal, introduced two years ago, captures stock prices and indexes from an FM radio wave, then displays them in a Lotus 1-2-3 spreadsheet format. Lotus says it won't fix the problem until the next release of Signal, and it won't say when that will be. Until then, Signal subscribers, who pay at least $100 a month for transmissions, will have to check that third digit -- or fourth -- in the next morning's paper.

> [Sounds like Signal has been Short-Sheeted. As the Father of the spreadsheet, maybe with Signal Lotus Leaves something to be de-Sired? (I suspect they do not anticipate another 100-point swing soon. Dow-dy?) Which digit is the Index finger? 1st in US, 2nd in Europe, 4th if you turn the right hand over. But having to check the fourth digit in the Dow-swing sounds really ominous! PGN]

Stark - warning depends on operator action, intelligence data quality

Jonathan Jacky <jon@june.cs.washington.edu>
Thu, 19 Nov 87 09:10:41 PST

The STARK's captain told the press some time ago that he thought the ship's warning system had not worked. It turns out the warning system is dependent on the quality of data loaded by operators. This information comes from John A. Adam, "USS STARK: what really happened?", IEEE SPECTRUM, Sept. 1987, 26 - 29. Some excerpts:

> Brindel, who had been the Stark's captain, said during a telephone interview on Aug. 5: "If the sensors that we had would have divulged the things they should have, then I'm sure my TAO (referring to tactical action officer Moncrief) would have taken additional measures." Brindel said neither the radars nor early warning receiver performed according to specifications. But he declined to elaborate, saying, "I think all the problems are being addressed by the Navy."
>
> Sources familiar with the Naval Board of Inquiry investigation have confirmed a statement by Brindel to SPECTRUM: the SLQ-32 radar receiver did detect the missiles coming but it failed to properly identify them. This is reminiscent of the (attack on the Sheffield in the 1982 Falklands War...) ...
>
> The SLQ-32 computer compares the observed signal characteristics with the parameters of possible radar emitters stored in the computer's library of friendly and hostile targets. When identification is complete, the computer sends it to the display to alert the operator.

...Identification as friend or foe can be "heavily influenced by the SLQ-32 operator" using software libraries. Some libraries, such as those for Soviet equipment, are fixed and cannot be tampered with; others, such as those for weaponry of US forces or Third World nations, are variable, allowing inputs from the operator when the ship is deployed in a given territory. One source familiar with the operations said the US military uses an "electronic order of battle" which lists all anticipated friendly, neutral, and hostile emitters. This, he said, would be the basis for SLQ-32 entries for a specific operation or region.

Thomas F. Curry, associate deputy assistant secretary for the Navy until 1983, said "it's probably more difficult to get intelligence information on friendly neutrals (like France or Iraq) than on hostile countries." ... Friendly neutral countries do not freely give information on their weapons to allies, since it would hurt military export sales. The US Navy had (conducted tests on some Exocets but) the Exocet's Paris-based manufacturer, Aerospatiale, refused to say whether it had recently changed the characteristics of the missile's seeker.

"Task Force Slams DoD for Bungling Military Software" (SDI, Ada, ...)

Jonathan Jacky <jon@june.cs.washington.edu>
Wed, 18 Nov 87 21:30:43 PST

Task Force Slams DoD for Bungling Military Software Efforts
ELECTRONICS, Nov. 12, 1987, p. 121.

The Defense Department's efforts in sofware development are disjointed, uncoordinated, and lack support, charges the Defense Science Board's Task Force on Military Software. The task force reports "it is convinced that today's major problems with military software are not technical, but management problems." It lambastes the DOD for having "not provided the vital leadership needed" in Stars, the Software Technology for Adaptable, Reliable Systems. It complains that Ada, the high-level programming language the DOD is pushing to make a standard for all military systems "has been overpromised." It warns that "the Strategic Defense Initiative has a monumental software problem" and that "no program to address the software problem is evident." To solve the management problem, the task force urges the DOD to bring together Stars, Ada, and the Software Engineering Institute under the Air Force Electronic Systems Division. It also wants representatives from the three programs and from the Defense Advanced Research Projects Agency's Strategic Computing Initiative to produce a "one-time jont plan to demonstrate a coordinated DOD Software Technology Program." What does the DOD have to say? Not much just yet. Officials at the Ada Program office did not respond to calls, and a DARPA spokesman would say only that the agency "has no plans to implement any of the changes the report recommends" at this point but will take them under consideration.

Addressable CATV (RISKS-5.61)

Jerome H. Saltzer <Saltzer@ATHENA.MIT.EDU>
Fri, 20 Nov 87 02:10:17 EST

Allan Pratt raises several good questions about privacy vis-a-vis addressable CATV technology, with the following starting point:

> The cable company serving the community where I live is upgrading
> their service to new, addressable converter boxes.

It turns out that the term "addressable" in the CATV industry almost always means "one-way addressable".

One-way addressable is moderately harmless to privacy--it really means only that the converter box responds to signals specifically addressed to it (such as "allow this customer to watch Showtime"). In a one-way addressable system there isn't a return path from the converter back to the head-end, so the company has no way of knowing whether or not the box responded, how many movies you have watched on the Playboy channel, or whether or not you have used the "mute" feature. The only things the company knows are what channels it tried to authorize, how promptly you pay your bills, and how often you complain about the service. There is still a good privacy issue, because their computer can easily generate for sale a mailing list, e.g., of everyone who subscribes to one of the premium sports channels. In our community, the CATV operator sends a yearly notice to each subscriber promising not to use CATV billing information for anything other than billing.

Although the FCC has for several years been requiring that new CATV systems be two-way capable, almost none of them actually implement the capability, because the technology is some distance over the edge of what the average CATV operator can keep running.

An operator probably wouldn't go to the trouble of shaping up his or her plant for two-way unless a big revenue stream is in prospect. The only revenue stream currently in prospect is pay-per-view. Two-way pay-per-view systems can be easily identified: if you can agree to pay for a pay-per-view event simply by pushing buttons on the converter box, it is two-way, and you should worry a lot about the problems that Pratt raises. If you have to call the cable company on the phone to "order" the pay-per-view event, they are using a one-way system, and you have some control over what they can know.

Last I heard a count there were perhaps twenty cable companies in the country running two-way, and the number was declining. Warner in Columbus, Ohio (under the name QUBE) is the most well-known.

Jerry

Human automata and inhuman automata

Chris Rusbridge <munnari!max.sait.oz.au!cccar@uunet.UU.NET>
Wed, 18 Nov 87 10:00:14 cst

There was a radio news item this morning about a Canberra company who received a Telecom bill over 2,000 pages long. Most of the pages

contained zero items, so I don't think they were complaining about the bottom line. However the bill was a stack of paper over 450mm high!

Of course, changes to Telecom's billing computer system were blamed for the debacle, which I think reached Parliament. The RISK illustrated here, above the common failures to test changes in production systems properly, is the human automaton who wrapped that stack of paper up in a parcel and sent it off, apparently without checking or reporting it. What kind of *human* system have they designed in there?

Chris Rusbridge, Academic Computing Service Manager
S. A. Institute of Technology
ACSnet: cccar@max.sait.oz
Phone: +61 8 343 3098 Fax +61 8 349 6939 Telex: AA82565
Post: The Levels, SA 5095 Australia

Re: CB frequencies and power

<dan@WILMA.BBN.COM>
Thu, 19 Nov 87 10:24:52 -0500

> CB's run at 4 Watts. Their wavelength is 436 inches. (~11m).
> JOHN MCLEOD Georgia Insitute of Technology, Atlanta Georgia

4 watts is the legal limit (power to antenna, as I recall), but when I was an amateur radio operator, it was common knowledge that CB'ers often flouted the law. They'd buy a ham amplifier for 10 meters and use it for 11 meters. They'd get 100-1000 watts that way (1kw being the legal ham limit). In cars, even.

So despite the low legal power limit on CB transmissions, it would not surprise me to hear of computer (and other) problems being caused by CB radios at a considerable distance.

Dan Franklin

Re: CB frequencies and power

John McLeod <jm7@pyr.gatech.edu>
Thu, 19 Nov 87 15:28:59 EST

This is true, however, after a few people got caught and had to pay $10,000 and up fines for running large amplifiers, a large number of those breaking the law stopped. More recently, however, there has been no enforcement at all on CB channels.

CB frequencies and power (RISKS-5.60)

Wm Brown III <Brown@GODZILLA.SCH.Symbolics.COM>
Thu, 19 Nov 87 14:19 PST

CB's run at 4 Watts. Their wavelength is 436 inches. (~11m).

That's the theory. In practice, however, *MANY* CB operators run bootleg power amplifiers which put out tens, hundreds, or sometimes thousands of watts. When computer-controlled engines started showing up on our roads, some truckers actually made a game of stalling them out by keying up CB transmitters nearby. Points were scored according to the performance/price class of the vehicles disabled and the degree of panic induced by engine failure at 65 MPH. VW drivers who wouldn't let an 18-wheeler pass them were targets for more serious electronic warfare -- it wasn't the trucker's fault that the VW stalled two car lengths in front of him....

The FCC has very few enforcement agents, and has pretty much given up any pretense of controlling the 27 MHz band. In some areas, owners of very high-powered transmitters establish 'ownership' of a CB channel by simply blasting everyone else off the air. An account of one Blackhawk crash laid the blame to a nearby 'bootleg CB transmitter,' which I interperted to mean one of these power mongers. The term "Alligator" has been coined to describe radios with "Big mouths and tiny ears."

Re: "UNIX setuid stupidity"

David Phillip Oster <oster%SOE.Berkeley.EDU@jade.berkeley.edu>
Wed, 18 Nov 87 08:14:33 PST

Thank you for the correction. The setgid solution is much better than the one I proposed. i didn't hit upon it because your solution does not solve the problem _as stated_ (Student creates a copy in the teacher's directory that no othe student can read.) Although it solves the more general problem. A still simpler solution: mail the assignment to the teacher.

--- David Phillip Oster --A Sun 3/60 makes a poor Macintosh II.
Arpa: oster@dewey.soe.berkeley.edu --A Macintosh II makes a poor Sun 3/60.
Uucp: {uwvax,decvax,ihnp4}!ucbvax!oster%dewey.soe.berkeley.edu

---

"UNIX setuid stupidity" (RISKS-5.57)

Stephen Russell <munnari!basser.cs.su.oz.au!steve@uunet.UU.NET>
19 Nov 87 10:54:10 GMT

In RISKS 5.57, David Oster makes the mistake of assuming that, as I reported the error concerning inappropriate use of a setuid root program, that I was responsible for it. In fact, the error was made by a member of the teaching staff (since left here) several years ago. While the member of staff probably should have known better, his attempts at making the program secure were naive. What is more worrying is that the program must have been installed by a system administrator, who certainly should have known better. This raises the interesting question of who is responsible for this security bug - the person who wrote the buggy program, or the programmer who installed it without vetting it?

(As an aside, Mr Oster's defamatory statements, accusing me of stupidity, illustrate how the immediacy of electronic mail tempt us to make comments which we would think twice about if actually face to face. Another computer risk?).

[I have omitted some of David's message, and ten or so additional messages on setuid/getuid. Most of them focused rather too narrowly on specific partial implementations, but missed the bigger picture. By the way, I do not normally run messages with personal implications, but this one seemed appropriate to clear the air. I imagine in this case one party may have been less than objective and the other may have been overly defensive. At any rate, the debate is deemed ended. PGN]

Software Safety Specification

<mlbrown@nswc-wo.ARPA>
Mon, 16 Nov 87 16:19:26 est

I am in the process of writing a draft MIL-SPEC for Software Systems Safety (MIL-SPEC-SWS). It is based on MIL-STD-SNS (draft) and will address the 300 series tasks from MIL-STD-882B and parallel the DoD-STD-2167 software development process. I am looking for suggestions for materials or subjects that should be included in the SPEC. Analysis techniques, specific topical areas that should be covered, etc. I would welcome any material that the RISKS readers would care to contribute. MIL-SPEC-SWS will be more of a how-to and guidelines document than a policy and what-to document. You can e-mail to me directly at mlbrown@nswc-wo.arpa or by conventional mail

Commander, Naval Surface Warfare Center
Code: H12 (M. Brown)
Dahlgren, VA 22448-5000

Thanks, Mike Brown

Call for Papers, COMPASS '88

Frank Houston <houston@nrl-csr.arpa>
Thu, 19 Nov 87 09:22:48 est

CALL FOR PAPERS

COMPASS '88
(Third Annual Computer Assurance Conference)

* A man with cancer is killed because a computer tells a radiation therapy machine to administer a lethal dose.

* A rocket on the way to Mars has to be destroyed because a crucial line is left out of the computer software controlling it.

* A bank is forced to borrow $23.6 billion overnight because of a computer, and the government-securities market narrowly escapes disaster.

* Workers are killed by computer controlled industrial robots.

All of these disasters have happened, and their numbers are increasing year by year. COMPASS is an organization dedicated to finding ways of combatting this problem, and increasing Computer Assurance. The name "COMPASS" combines abbreviations of "COMPuter" and "ASSurance".

What do we mean by computer assurance?

One might define the term analytically by including process security, systems safety, software safety, reliability, quality control, testing, verification and validation, mathematics, physics, and various engineering disciplines. It is not, however, a simple combination of these. On the one hand, a system may be totally unreliable yet perfectly safe; on the other hand, a safe system may sometimes not be an appropriate goal. Furthermore, there are deep, unresolved philosophical questions about both immediate design goals of autonomous systems and more universal meta-goals apropos of dealing with the unexpected. What should these goals be and how do the design goals and the meta-goals interact?

Help us explore computer assurance, define its boundaries, identify its issues, and realize its objectives. Submit an article or abstract for the 1988 conference.

Abstracts of any length will be considered; complete papers are preferred. All submissions should be typed double spaced and single sided (draft form). Upon acceptance, IEEE kits for preparing camera ready copy will be sent.

```
  ======================================================================
                          *
  Dates:  27 June -- 1 July '88     *  Mail manuscripts, abstracts and
                          *  requests for information to:
   Location:  Washington, D.C.      *
      ---------------           *
General Chair: CDR Micheal Gehl, ONR *          COMPASS '88
                          *         P.O. Box 5314
 Program Chair: Janet Dunham, RTI   *       Rockville, MD 20851
      ---------------           *
  Submissions due:  30 Jan 1988     *  ( ) Submission  ( ) Information
                          *
  ======================================================================
```

Submit abstracts electronically to Janet Dunham (jrd@rti.rti.org).
For more information contact Frank Houston (houston@nrl-csr.arpa).
Be sure to include your mailing address.

"Normal Accidents" revisited

David Chase <acornrc!rbbb@ames.arpa>
Thu, 19 Nov 87 8:37 PST

I just finished "Normal Accidents" by Charles Perrow (Basic Books, 198?). I recommend it for your class and I recommend it for RISKS aficionados. Perrow's thesis is that "complex, tightly-coupled systems" will have accidents; the accidents are "normal". He also writes about risk-inducing organizations and the way that they "analyze" accidents ("blame the operator" is a common theme--certainly it has low short-term cost, and avoids the inference that (say) nuclear power is intrinsically disaster-prone).

He says little about computers in this book. However, he provides enough examples of unexpected interactions and multiple errors to make most people hesitant about claiming to "cover all the bases" (e.g., I did not know that dams could cause the earth beneath them to shift, though it makes perfect sense in hindsight).

David Chase, Olivetti Research Center, Menlo Park

[This book is one of the cornerstones of RISKS, and is worth noting here again every now and then, particularly for new readers. PGN]

Space Shuttle Whistle-Blowers Sound Alarm Again (reprint)

<rdicamil@CC5.BBN.COM>
Thu, 19 Nov 87 18:16:45 -0500

Space Shuttle Whistle-Blowers Sound Alarm Again
(Electronic Engineering Times, 11/16/87)

by Richard Doherty

HOUSTON - The first step in a concerted action by so-called technology whistle-blowers to increase public awareness of continuing problems with the NASA shuttle will be made here this week.

On Wednesday, former Lockheed company engineer John Maxson is due to address an ethics meeting of the American Society of Mechanical Engineers about the wider aspects of whistle-blowing. During his presentation, Maxson is expected to give evidence collected over the past few months that he will claim supports fears that critical shuttle sub-system problems still remain.

Maxson will share the stage with former Morton Thiokol engineer Roger Boisjoly, who currently has a billion-dollar suit underway against his one-time employer and NASA. Boisjoy has charged that Morton Thiokol conspired to cover up problems with the shuttle's solid rocket motors, the failure of which was blamed for the Challenger tragedy last year. He also claims he suffered personal injury as a result of the disaster.

Boisjoly was one of several Morton Thiokol engineers who objected to the launch of the Challenger before its ill-fated liftoff.

Maxson was dismissed by Lockheed's Space Operations Co. some months after the shuttle was destroyed. Six weeks before the shuttle explosion, in December 1985, Maxson had tried to convince Senator Charles Grassley

(R-Iowa), a supporter of such whistle-blowing, that problems with the shuttle launch system should preclude the launch of the shuttle Columbia.

Columbia, which lifted off successfully after a near-disastrous mistake in fueling liquid oxygen tanks, was the last successful shuttle launch.

Maxson has sued Lockheed for wrongful dismissal, and claims he is one of hundreds of NASA and contractor employees who were forced out "for doing our jobs".

In coming months, as more evidence surfaces, Maxson aims to rally support among other unemployed engineers. He hopes to help restore their jobs and also raise industry awareness of shuttle subsystem problems and managerial laissez-faire attitudes that he claim threaten a scheduled safe return to space June 2.

My addendum comment: As a usual watcher of CNN "headline news" I've noticed lately some press about another "new shuttle escape system". This one is some kind of rocket designed to pull (a parachuted equipped) astronaut out of the ship by a harness. I did notice that CNN mentioned in their commentary that this kind of escape system would not have saved the astronauts in the Challenger disaster. However, I have failed to hear such commentary included in similar stories of the major networks.

Too, this is one recent story in a seemingly continual series of press releases about the new and improved shuttle escape mechanisms. Lot's of money is being spent, but whether reported or not, upon (close) examination none of these mechanisms would prevent the death of astronauts in a Challenger type disaster.

I wonder just how much additional engineering is happening for purely public relations purposes (and at what, if any risk) ? Perhaps this is just another clever manifestation of the "laissez-faire" attitude Mr. Maxson is trying to expose. It's unfortunate that such P/R, spaced even over many months, could lull the public into a false sense of security. Also, such news less any critical commentary - does sell quite well (news reporting is also a commodity).

Search RISKS using swish-e

THE RISKS DIGEST

Forum on Risks to the Public in Computers and Related Systems

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

Volume 5: Issue 63

Monday, 23 November 1987

Contents

Logic bombs and other system attacks -- in Canada

Peter G. Neumann <Neumann@KL.SRI.COM>

Mon 23 Nov 87 13:27:25-PST

An article by Kirk Makin in the Globe and Mail, 3 November 1987, describe a talk given by Sergeant Ted Green of the Ontario Provincial Police at the recent annual conference of the Probation Officers Association of Ontario.

* A disgruntled employee of a London, Ontario, company planted a logic bomb that would have knocked out the computer system. It was detected. The man was prosecuted, but not convicted. Evidence of a previous logic bomb implantation was not admitted because the previous company (in Alberta) had refused to press charges.

* Another Toronto company had a logic bomb triggered the day an employee's termination notice was processed by the computer system. Sgt Green noted that "It wiped out the whole system."

* On the occasion of its 10th anniversary, a bank branch decided to honor the customer who had the most active account. It turned out to be an employee who had accumulated $70,000 funnelling a few cents out of every account into his own.

* On employee altered an access password and demanded $50,000 to reveal the new password. Apparently he got it.

* One Toronto student recently made 2177 attempts to enter the computer system of Alcan Aluminium's Kingston, Ont., plant.

Sgt. Green also noted $1000 in computer-initiated bogus charges, a[nother] bogus bank deposit slip scam attempt, and a case of a Toronto-area machinery supplier using mailing lists and blueprints extracted from a rival's computer.

Video signal piracy hits WGN/WTTW

Rich Kulawiec <rsk@s.cc.purdue.edu>
Mon, 23 Nov 87 17:20:56 EST

At about 9:15 CST last night (Sunday, November 22, 1987), "superstation" WGN-TV (Channel 9 in Chicago) was the victim of an interesting technological crime; its signal was overridden for approximately 15 seconds by a pirate transmission. The incident was repeated at about 11:15 CST, with WTTW (Channel 11, the Chicago PBS station) falling prey on the second occasion, which lasted about 90 seconds.

The transmission, which interrupted a newscast on WGN and "Dr. Who" on WTTW, consisted primarily of someone in a Max Headroom mask throwing Pepsi and Coke cans around while raving in a largely unintelligible voice. The transmission concluded (I'm not kidding) with a shot of the Max-impersonator's exposed derriere' being whacked with a flyswatter. The video quality of the transmision was fairly good, but the audio was very garbled. I happened to be taping Dr. Who at the time, and so I've watched the broadcast several times; even so, I can't understand more than a word or two.

A couple of phone calls (to the local cable TV company, and to WTTW) led to a little more information; it is likely that the pirate transmission was inserted somewhere in the Chicago area, as it was distributed over WGN's satellite link and WTTW's (land-based) microwave links. If my information is correct, WGN has the capability of switching to a second frequency for the uplink portion of its broadcast chain, but it's not clear whether they actually did so during or after the incident. WTTW does not have this capability, and the person I talked to on the phone sounded (understandably) a little worried that this might happen again.

As one might expect, the FCC and the FBI, among other agencies, are investigating. It seems likely to me that the culprit found a point through which WGN's and WTTW's signals both pass, and tapped in at that point; while this certainly isn't the only way that this piracy could be accomplished, it seems the easiest.

Rich Kulawiec, rsk@s.cc.purdue.edu, s.cc.purdue.edu!rsk

[This is becoming almost too frequent, but still worth noting. PGN]

Garage Door Openers

Brint Cooper <abc@BRL.ARPA>
Thu, 19 Nov 87 11:40:39 EST

This morning's Baltimore Sun tells of folks in Frederick, MD, who are having great difficulty with their remotely controlled garage door openers. It seems that, installed in their houses, these things have just stopped responding to commands from the hand held unit. However, when taken back to the point of purchase, they work just fine.

The U.S. Army has an installation, Ft Detrick (sp?) nearby. One of its two functions has something to do with electronic communications. An Army spokesperson denies that the Army is radiating anything that would lock up these receivers.

_Brint

Sudden acceleration revisited

Nancy Leveson <nancy@commerce.UCI.EDU>
Mon, 23 Nov 87 08:50:21 -0800

There was just a report on the NBC news (Sunday, Nov. 21 at 4:30 pm PST) on the sudden acceleration problems with the Acura Legend. The Acura dealers say it is driver error. The drivers all say they have been driving for 30-40 years without an accident or a ticket and they insist they had at least one foot on the brake (one woman said she had both feet on the brake). A mechanic who has been examining one of the cars involved says it is obviously a problem in the fuel injection system, and he is sure that the computer is involved.

Does anyone know if there is any connection between the microprocessor used in the Acura and in the other cars with this problem, e.g., the Audi 5000?

Centralized Auto Locking

"Lindsay F. Marshall" <lindsay%kelpie.newcastle.ac.uk@NSS.Cs.Ucl.AC.UK>
Mon, 23 Nov 87 11:19:20 GMT

My father spotted a report in a paper about someone who was trapped in a car when the central locking mechanism went haywire. The person in question was too large to escape by climbing through the window, which was how some of the other passengers got out. Sadly I have no more details about this as my father couldn't remember where he had seen it - it sounds like a FOAF story ("friend of a friend" story - urban legend, if you're a sociologist), but I'd be interested if anyone else has heard it.

Lindsay

Re: The Stark incident (RISKS DIGEST 5.62)

Amos Shapir <nsc!taux01!taux01.UUCP!amos@Sun.COM>
22 Nov 87 09:38:59 GMT

It looks like the culprit in this case was whoever decided to classify incoming missiles into 'hostile' and 'friendly' categories - did they think that a friendly missile fired by mistake should behave any friendlier than a hostile one?

Amos Shapir (My other cpu is a NS32532)
National Semiconductor (Israel)
6 Maskit st. P.O.B. 3007, Herzlia 46104, Israel Tel. +972 52 522261
amos%taux01@nsc.com (used to be amos%nsta@nsc.com) 34 48 E / 32 10 N

Bank Networks (Re: RISKS-5.61)

George Bray <lcc.ghb@SEAS.UCLA.EDU>
Fri, 20 Nov 87 13:02:58 PST

I have two comments on the article in RISKS 4.61 by David G. Grubbs:

>(VISA card numbers all start with 4, Master Card with 5, AMEX with 37, etc.)

Actually, AMEX cards can begin with 34, 35, or 37. (Nit-picky, I know.)

> Our money is managed by people who care nothing for the details of
> an single transaction. They sell financial services like the grocer
> sells apples. So what if a few are dropped on the floor? It's just a
> "cost of doing business." As the throughput of transactions increases over

> time, each detail gets commensurately smaller. It can only get worse.

That is quite true. In my days working for a bank (which actually was better than most about it) I was often astounded at the cavalier attitude towards a single transaction. Of course, from the point of view of the bank, fixing a major problem in the middle of the day (one that was costing thousands of dollars an hour) is clearly vital, but I couldn't help worrying about the poor customer who happened to go up to an ATM during the 10 minutes the front-end processor was being downloaded, or during any other downtime in the middle of the day. From the bank's point of view, a few transactions lost out of half a million or more a day is minor. From the customer's point of view (who is late for a flight and needs cash), that one transaction is critical.

George Bray

Re: Optimizing for cost savings, not safety (RISKS-5.57)

Dave Horsfall <munnari!runx.ips.oz.au!dave@uunet.UU.NET>
Sat, 21 Nov 87 01:33:04 AESST

> Re: Optimizing for cost savings, not safety (John McLeod)
>From: bill@trotter.usma.edu (Bill Gunshannon)
> A letter was published in an amateur radio oriented magazine called QST
>a few years back by a ham who tried to install a UHF mobile radio in his
>newly purchased Japanese import. He too had problems with interference to
>the electronic ignition in the car. A call to the US Service Representative
>for the cars manufacturer resulted in a very simple solution to the problem.
>They told him "don't install the radio in the car".
>
> A novel approach to preventing interference.
> bill gunshannon

Another "informed" reply that appeared in an amateur radio magazine was: "Try shielding the antenna". And these people design cars?

-- Dave

L.A. Earthquake & Telephone Service

"LT Scott A. Norton, USN" <4526P%NAVPGS.BITNET@wiscvm.wisc.edu>
Fri, 20 Nov 87 15:17:09 PST

The December 87 issue of The Institute: News Supplement to IEEE Spectrum has a short but interesting article on the effect of Oct 1st's Los Angeles earthquake on the utilities. Most of the article deals with electric power, which had the most problems (but still minor). But a few paragraphs on the telephone service should be of interest to RISKS readers.

The article points out that telephone network was largely undamaged by the quake because many lines have recently been replace by fiber optic cables that were installed with a large amount of slack, which permitted them to move without breaking during the quake.

As we already know, many subscribers were unable to get dial tones after the quake. I thought "Lots of people calling relatives tied it up", which was a factor, but The Institute reports that most of the delays resulted because the quake knocked phone receivers off the hook. Of course, anxious and curious callers also tied up the lines, and two central offices lost power intermittently.

Can anyone with better knowledge of the phone companies' local offices tell me if there is some simple way to shed this extra load in a reasonable way? I know that after some minutes off the hook, the phone loses its dial tone. Does this adequately release the resources the off-the-hook phone was using?

LT Scott A. Norton, USN | From Internet, if you need a gateway, use
Naval Postgraduate School | 4526p%navpgs.bitnet@jade.berkeley.edu
Monterey, CA 93943-5018 | or 4526p%navpgs.bitnet@ucscc.ucsc.edu
4526P@NavPGS.BITNET | The WISCVM gateway will close 15 Dec 87.)

Gripen flight delayed

<mnetor!utzoo!henry@uunet.UU.NET>
Tue, 17 Nov 87 21:04:31 EST

The Oct 5th Aviation Week reports that first flight of Sweden's new Gripen fly-by-wire combat aircraft will slip about eight months due to software development delays. This is on top of a previous six-month slip for the same reason. This is the last slip that can be absorbed without delaying the operational service date (1992). No real details were provided; on the surface it would appear that things are going well but unexpectedly slowly, and prime contractor Saab-Scania is just being cautious.

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

> [Yes, this is a risk commonly attributed to computers, but it is hardly novel. It is included to remind us of the dependence on the software development process... PGN]

Mariner 1

Mark Brader <msb@sq.com>
Sun, 22 Nov 87 12:34:05 EST

> * A rocket on the way to Mars has to be destroyed because a crucial line is left out of the computer software controlling it.

Presumably the above refers to Mariner 1. This is about the fourth or so version that I've heard of what the actual error was. Arthur C. Clarke says it was a missing "-". Others say that a "." was typed in place of a "," in a Fortran DO statement (thus turning it into an assignment).

Peter, do you know of a reference that tells authoritatively what the actual

bug was? Normally I'd consider ACC authoritative, but the version he tells doesn't seem to appear anywhere else, so maybe not this time.

I posted the same question to sci.space a year or two ago and got no takers.

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

[We've tried this one before, but perhaps someone new has joined us. PGN]

Systemantics

John Gilmore <hoptoad.UUCP!gnu@cgl.ucsf.edu>
Sat, 21 Nov 87 06:32:18 PST

David Chase's recommendaion of "Normal Accidents" reminded me of the book "Systemantics" which I read years ago and can no longer remember the vitals of. Its premise, well explored and humorously explained, is that sufficiently complex systems always have unexpected behaviours.

I suspect it's another RISKS cornerstone.
John Gilmore

["Systemantics" by John Gall. Although humorous, in the spirit of Parkinson's Law, it has some great truths, such as

"Fail-safe systems fail by failing to fail safe."

haynes@ucscc.bitnet, ...ucbvax!ucscc!haynes]

[Legendary! Previously noted in RISKS by
Jim Horning, RISKS-1.2;
Earl Boebert, RISKS-2.16;
Hal Murray, RISKS-2.18.
Consult your local Books-in-Print. PGN]

Re: "UNIX setuid stupidity" (RISKS-5.57)

"Joseph G. Keane" <jk3k+@andrew.cmu.edu>
Sat, 21 Nov 87 10:51:03 -0500 (EST)

The designers of UNIX considered that a trusted program may wish to allow operations only on a certain part of the directory tree. So they provided the `chroot' system call, which allows a program to do just that, in a secure way. I was surprised as i saw the argument go by with no one mentioning this, but maybe i shouldn't have been. I guess the moral is that a feature doesn't do you any good if no one knows about it.

--Joe

<minow%thundr.DEC@decwrl.dec.com>

(Martin Minow THUNDR::MINOW ML3-5/U26 223-9922)
Date: 23 Nov 87 09:02
To: risks@csl.sri.com
Subject: further comment on setuid problem

From Risks 5.62:
>From: munnari!basser.cs.su.oz.au!steve@uunet.UU.NET (Stephen Russell)
...
>This raises the interesting question of who is responsible for this security
>bug - the person who wrote the buggy program, or the programmer who
>installed it without vetting it?

Perhaps one might add to this list the people who designed an error-prone capability, or the people who failed to document the way in which a security-enhancing function can -- though used with good intent -- serve to decrease the security of the system.

Martin.

Search RISKS using swish-e

THE RISKS DIGEST

Forum on Risks to the Public in Computers and Related Systems

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

Volume 5: Issue 64

Tuesday, 24 November 1987

Contents

More on NASA Hackers

Dave Curry <davy@intrepid.ecn.purdue.edu>
Tue, 24 Nov 87 10:36:28 EST

Some of this information has already been covered in RISKS and elsewhere, but this article does a fairly good job of summing up both the original problem and DEC's response to it. (Dave)

Quoted without permission from "Digital Review", November 23, 1987, page 80.

NASA Hackers: There's More to the Story
Vin McLellan

More details have come to light regarding the attack this summer on NASA's Space Physics Analysis Network (SPAN) by the young German hackers known in the European press as the "Chaos Computer Club".

SPAN is a large, VAX-based network for scientists in the United States and other countries who wish to exchange unclassified information on post-flight space studies. According to NASA officials, SPAN links about 800 computers in government, industry and academe.

The SPAN network suddenly became well known after the Chaos hackers held a press conference in Hamburg, West Germany, earlier this fall to decry the lax VMS security that had allowed them to penetrate 20 different SPAN systems in Europe and the United States.

NASA officials said the Chaos hackers had a considerably inflated idea of the value and confidentiality of the information stored on the SPAN systems. Although academic researchers may have labeled their files with eye-catching titles such as SDI_STUDIES, explained a NASA spokesman, there was no classified data stored on SPAN.

The hackers were, however, able to exploit a flaw in the VMS access control system. The problem was a bug in a VMS system software module called SECURESHR.EXE. DEC first learned of it last year, in late December, according to Andy Goldstein, a senior engineer in DEC's VMS group. The bug was subtle but serious, he said. It allowed a sophisticated hacker to gain privileges from a normally unprivileged account. DEC, said Goldstein, had a "fix" available by early February, "a little slower than usual because of the holidays."

The Chaos hackers were able to exploit the delay between the early reports of the problem and the later distribution and implementation of DEC's corrective patch. Although DEC's U.S. and European support centers had the patch available on request in February, Goldstein said, it wasn't until June or July that DEC issued a VMS "special release" to deal with the problem. And even then, there were users who should have received the patch but didn't.

The patch to SECURESHR.EXE "took a long time in coming to Europe," complained Roy Omond, EDP manager at the European Microbiology Lab (EMBL) in Heidelberg, Germany. At EMBL, the delay was costly. "Before I had the chance to install the [SECURESHR] patch," Omond said, the Chaos Club had invaded his system. When he realized what had happened, he broadcast an angry warning over SPAN and Arpanet.

The Chaos hackers patched two VMS images, SHOW.EXE and LOGINOUT.EXE, explained Omond. Those patches modified the system to install both a VMS "trap door," which let hackers access the system at any time using their own magic password, and a "password grabber" to collect and record the passwords of legitimate users.

"Given that these were modifications to the trusted VMS software," Goldstein noted ruefully, "there was nothing that you could do to defend against them."

The LOGINOUT patch was "lethal," Omond said. "Not only would it allow entry to any user name with the magic password, but it would also store valid passwords of all users logging in since the patch was installed." The passwords were stored in the 12 bytes reserved for customer use in each User

Authorization File (UAF) record. The hackers have a small program that retrieves the user name/password pairs from the UAF, he said, neatly printing them out with an asterisk next to the name of each user with privileges.

The Chaos code also corrupted the VMS accounting system, Omond said. Even when hackers were logged in, they would not appear on a job count or be listed with a SHOW USERS command.

"They have cost us a lot of real money by using our X.25 connection to log in to several places all around the globe," Omond said. "I have done my best to notify... the VAX sites that were accessed from our hacked system. I pray that no other damage has been done, and that I am not sitting on a time bomb."

Omond hid neither his fear nor his anger. He published the names of three people whom he accused of circulating the Chaos code - at least two of them were apparently employees at SPAN sites - in the hope, he said, that "someone somewhere will (a) be saved some hassle from them, and (b) might perform physical violence on them."

Re: Video signal piracy hits WGN/WTTW

Will Martin -- AMXAL-RI <wmartin@ALMSA-1.ARPA>
Tue, 24 Nov 87 14:55:14 CST

For what its worth, the explanation of this incident that I saw on the evening newscasts cited the method as being an overriding of the studio-transmitter microwave link by a higher-effective-power transmitter. They illustrated this with a drawing showing a vehicle with a microwave dish on it pulled up close to the building atop which the transmitters are located, and that dish aimed at the microwave receiving antennae mounted on that building. That could be expected to put higher effective power into that receiver, and some form of "capture effect" would allow this interfering signal to override the normal legitimate input signal coming from the studio.

Of course, there are problems with this -- how would it have affected the satellite-relay of WGN, for example, unless that is taken from an off-the-air signal at the uplink site (which seems an unlikely arrangement)? Same about the microwave land-relays for the PBS station; one would have thought both of those would travel from the studios to various other sites directly. (Perhaps, though, the high-building transmitter site is also a point of origination for microwave relays to other places, and the pirate overriding the input fed his signals into both the broadcast transmitter and the outgoing microwave relay chains?)

The other main problem that occured to me is that it would probably be too obvious and visible to do this. However, now that I think about it, could it have been done from behind a glass window in another tall building around that site? That could be just about undetectable if it is possible. I've been at the transmitter end of such microwave studio-transmitter links where the dish antenna was inside the room, facing directly at an ordinary studs-and-plywood wall. That wall was essentially invisible at those frequencies. (Since this was on top of a mountain, it sure made maintenance easier, keeping the gear out of the weather!) So if one could

do this from an office or apartment in a nearby high-rise, behind a curtain and through a closed window or glass wall, the only way to locate it would be to DF the signal while it was actually transmitting. If the pirate kept to short unpredictable bursts, this wouldn't be feasible.

I suppose the studio-transmitter link could be encrypted, but it would still be subject to disruption by this technique. Though this would prevent a pirate from getting a recognizable signal out over the transmitter, his override would keep the legitimate signal from getting through. They would have to go back to landline to avoid that.

Regards, Will Martin

[Rich Kulawiec (rsk@s.cc.purdue.edu) submitted an article by John Camper (and Steve Daley) from the front page of the Chicago Tribune, 24 Nov 87. The article adds details to what Rich contributed to yesterday's RISKS-5.63, but nothing of real relevance to RISKS. Most of you probably saw similar write-ups in your local rags. PGN]

Logic Bombs; Centralized Auto Locking (RISKS-5.63)

P. T. Withington <PTW@DIAMOND.S4CC.Symbolics.COM>
Tue, 24 Nov 87 12:24 EST

Logic bombs et al.: The version I read [of the $70,000 salami attack] was that, when discovered, the employee threatened to expose that the bank had previously been funneling the same "roundoff" into its own profits and that he went unpunished on his promise to keep quiet. (On the other hand, the "banks get rich on roundoff" tale is an old computer-fraud chestnut, ranking right up there with the alligators in the NYC sewers.)

Centralized Auto Locking: I know a friend whose battery went dead and hence he couldn't unlock his car to open his hood! (Of course the tow-truck operator easily "jimmied" the door lock.)

Re: Mariner 1

<utzoo!henry@uunet.UU.NET>
Mon, 23 Nov 87 16:03:01 EST

Oran W. Nicks, in "Far Travellers" (NASA SP-480) states that Mariner 1 failed because of a combination of two problems. ... And there was a hyphen missing from the internal guidance software. ... Nicks was Director of Lunar and Planetary Programs for NASA at the time, and I think we can assume that he knows what he's talking about.

By the way, Mariner 1 was bound for Venus, not Mars.

Mariner 1

<Mary.Shaw@sei.cmu.edu>
Tuesday, 24 November 1987 15:31:50 EST

In SEN 5,2 (April 1980), a letter from the editor on p. 5 said that it was Mariner 18 that was blown up because of a missing NOT in a program. I didn't note any further attribution.

[You can't always trust those editors. Besides, I'm not even sure there ever was a Mariner 18. PGN]

In RISKS-3.41 (August 1986), Alan Wexelblat reported that a Mariner probe to Venus was lost because a period replaced a comma in a FORTRAN DO statement (that is, something of the form DO 3 I=1,5 became DO3I = 1.5). Wexelblat attributed this report to an article in the Annals of the History of Computing, 1984 (6) 1, page 6; I haven't followed the pointer back.
Mary

[Andrew Taylor <ATAYLOR@ibm.com> reminds us of the reference (in RISKS-4.1) to Software Engineering Notes v8,5 and v11,5. The earlier one refers to the Annals of the History of Computing. I was hoping someone would turn up an independent source. PGN]

Mariner 1 or Apollo 11? (RISKS-5.63)

Scott Dorsey <kludge@pyr.gatech.edu>
Tue, 24 Nov 87 18:36:50 EST

I heard that the famous "./," disaster caused the problem with the onboard IBM 1800 on Apollo 11. I heard this from a professor who teaches Fortran, so I'm not so sure about the reliability of the source. Anyone else have information on either the Apollo or the Mariner problems?

Scott Dorsey Kaptain_Kludge
SnailMail: ICS Programming Lab, Georgia Tech, Box 36681, Atlanta, Georgia 30332
Internet: kludge@pyr.gatech.edu
uucp: ...!{decvax,hplabs,ihnp4,linus,rutgers,seismo}!gatech!gitpyr!kludge

---

Bank Transaction Control

Martin Ewing <mse%Phobos.Caltech.Edu@DEImos.Caltech.Edu>
Mon, 23 Nov 87 23:36:23 PST

"Our money is managed by people who care nothing for the details of an single transaction." [sic] (Grubbs, 4.61)

I had a friend who was employed as an old-fashioned bank teller a few years ago. From her report, it was an extraordinarily grinding, low-paying job. Error control consisted of making her personally responsible for any cash shortages at the end of the day. More than one or two discrepant days and she would be out on the street.

Was this strict supervision to protect the customers, or to prevent employee pilferage? You decide.

There seems to be no control in ATM systems that's quite comparable. Should programmers, maintenance people or DP execs be forced to make good any system losses?

Re: Sudden acceleration revisited

Donald A Gworek <gworek@codas.att.com>
24 Nov 87 13:32:45 GMT

Word of advice. If you find yourself in sudden acceleration and the brakes can't stop the car, try knocking the gearshift into neutral to disable the car.

Gearshifts are usually built with a feature where you can slip into neutral just by pushing the shifter.

I learned this technique in driver's ed several years ago to avoid getting into an accident if the gas pedal sticks to the floor. The engine will roar, but at least you'll be stationary or in control of the vehicle.

Don Gworek { gatech, ihnp4, mtune }!codas!gworek

Re: CB radio and power

Jeffrey R Kell <JEFF%UTCVM.BITNET@CUNYVM.CUNY.EDU>
Mon, 23 Nov 87 14:29:52 EDT

One addendum to the CB interference postings... CB is 11-meter, or more accurately beginning at the high end of 26Mhz and through 27Mhz. The big hazard of illegal use of 10-meter amateur amplifiers on 11-meter signals is you don't get the RFI reductions from the RF chokes and filters in the amplifier that are tuned to 10-meter. To defend the real amateur stations, they probably aren't generating a 'ludicrous' amount of RFI; but using the same rig at 11-meters loses the inherent filtering and you get lots of noise.

You have probably noticed car radio interference quite often on the freeways when the big trucks with 'alligator' radios pass by (depending on what station you are tuned to). The second harmonic of 26-27 Mhz signals rounds out to 104-108 Mhz, or the upper half of commercial FM radio.

More on Garage Doors

Brint Cooper <abc@BRL.ARPA>
Tue, 24 Nov 87 9:28:11 EST

This morning's Baltimore Sun reports that when certain transmitters at Fort Detrich were turned off, the garage door openers in residential Frederick, Maryland, began opening again. It continues that the Army remains non-commital regarding its responsibility in the matter but notes that Detrich is a major communications node for domestic and international traffic.

We should not miss the implied risk to computer systems (and, therefore, the risk to those depending upon computer systems) if such phenomena continue. Today, your garage door won't open; tomorrow, perhaps your PC won't boot.

_Brint

Train crash in Sweden [RISKS-5.60]

Matt Fichtenbaum <genrad!mlf.UUCP@seismo.css.gov>
24 Nov 87 14:27:55 GMT

[More on the head-on train crash on 16 Nov 87 in Sweden -- in which nine were killed and 120 injured.] Neither train was to stop in the station; one train, approaching the station at high (traveling) speed, suddenly found itself shunted over to the opposing track.

According to Swedish shortwave news, construction machinery had inadvertently cut a cable. When the cable was repaired two conductors were interchanged, causing the accident. The news report didn't clarify whether the cable error resulted in a switch being in the wrong position or a signal's incorrectly indicating "ok to proceed."

[I first read that as "two (train) conductors" were interchanged. PGN]

Re: L.A. Earthquake & Telephone Service

Darin McGrew <ibmpa!mcgrew@ucbvax.Berkeley.EDU>
Tue, 24 Nov 87 11:41:04 PST

>... I thought "Lots of people calling relatives tied it
>up", which was a factor, but The Institute reports that most of the
>delays resulted because the quake knocked phone receivers off the hook.

It seems to me that a telephone handset resting in the cradle of a heavy base with rubber feet stands less chance of ending up off the hook after an earthquake than the new telephones that simply rest on a flat surface.

Could this be a risk of the simple lightweight telephones?

Darin

[Comment on the whole issue: Some of the contributions have been somewhat picky lately, and quite redundant. Please observe the masthead guidelines. PGN]

Search RISKS using swish-e

Report problems with the web pages to the maintainer

Search RISKS using swish-e

THE RISKS DIGEST

Forum on Risks to the Public in Computers and Related Systems

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

Volume 5: Issue 65

Wednesday 25 November 1987

Contents

Mariner I and computer folklore

Jon Jacky <jon@june.cs.washington.edu>
Tue, 24 Nov 87 22:13:08 PST

Mark Brader asks what really happened to Mariner 1, the Venus probe that had to be blown up when it flew off course shortly after launch. Some versions of the story blame a missing hyphen, others blame a period substituted for a comma.

I looked into this about a year ago. I lost the trails of both versions without finding a common ancestor. Here is what I found out. I hope some reader can help. The anecdote is told so often that someone really ought to settle this once and for all.

> New York Times, July 23, 1962, p. 1 col. 2: Atlas carrying Mariner I goes off course, destroyed by range safety officers
>
> New York Times, July 28, 1962, p. 1 col. 4: NASA, USAF, JPL announce Mariner I lost because flight control computer generated incorrect steering commands. Problem described as a "missing hyphen."

New York Times, Aug 2, 1962, p. 24 col 5: Letter to the editor about Mariner I, calls for better computer programming practices.

Mariner I loss attributed to substitution of period for comma in FORTRAN program: Henry S. Tropp, "FORTRAN Anecdotes," ANNALS OF THE HISTORY OF COMPUTING, Vol 6, No. 1, Jan 1984 pps. 61,62. Tropp merely cites Jim Horning in ACM SOFTWARE ENGINEERING NOTES, 4(4) Oct. 1979 p. 6, who cites in turn G.J. Myers, SOFTWARE RELIABILITY: PRINCIPLES AND PRACTICES, New York, John Wiley, 1976, p. 275.

It looks like the missing hyphen version is much older. I haven't been able to trace the period-for-comma version to a printed source before Myers. Still, I am not ready to accept the hyphen version as authoritative. I don't have a copy of the NY TIMES story - I had to make notes from a microfilm reader - but I recall that it seemed a bit confused, as if the reporter did not quite follow the explanation he was given. Also, I seem to recall hearing the period-for-comma version long before Myers, when I was in college around 1970. Can anyone else offer an older citation?

A few leads I never followed up: obviously, Myers himself could to be contacted to learn where he got the story. I called IBM, credited in Myers' book as his place of employment. IBM said Myers had left some years ago and they had no forwarding address.

Also, RISKS Volume 1 number 2, 28-Aug-1985, included a posting from Nicholas Spies (Nicholas.Spies@CMU-CS-H.ARPA), in which he mentioned a memo about the incident which his father had seen at the time. No details were given in that posting. Nicholas, are you still there? Can you help?

I think this matter would make an interesting case study for a folklorist. It certainly has a lot of the aspects of the kind of urban folklore retold in the book THE CHOKING DOBERMAN or an FOAF story ("this happened to a friend of a friend"). In this case however, the tales are based on a real event in the fairly recent past, so it should still be possible to find out what actually happened.

It is interesting to note how a single incident gave rise to at least two incompatible versions. They now have an independent life - the RISKS index in ACM SOFTWARE ENGINEERING NOTES, 12(1) Jan 1987 p. 23 cites both versions as if they were two separate events. The versions continue to fracture into increasingly garbled variants. The announcement for COMPASS '88 in RISKS-5.62 said "a rocket to Mars had to be destroyed...". The index in SEN also mentions "Mariner 18 - aborted due to missing NOT in program". It is not clear where this comes from; possibly another Mariner 1 mutation, or maybe it is supposed to be Mariner 8, which my ILLUSTRATED ENCYCLOPEDIA OF SPACE TECHNOLOGY (by Kenneth Gatland, Harmony, 1984) says "was lost during launch." Whatever, there was no Mariner 18 - the last in the Mariner series was 10, a 1973 Venus flyby.

- Jonathan Jacky

[Jon, MANY THANKS. PGN]

Mariner/Annals [A little duplication and a little more clarification]

Jim Horning <horning@src.DEC.COM>
Wed, 25 Nov 87 13:14:04 pst

The reference to ANNALS OF THE HISTORY OF COMPUTING, vol. 6, no. 1, should be to page 61, not 6. However, it sheds little additional light: It quotes my note in SEN October 1979, and my reference [3], G. J. Meyers, SOFTWARE RELIABILITY: PRINCIPLES AND PRACTICES, John Wiley, 1976, p. 275. Meyers doesn't cite his source, and I have never been able to get independent confirmation.

Jim H.

Computer-controlled train runs red light

Jon Jacky <jon@june.cs.washington.edu>
Tue, 24 Nov 87 22:16:54 PST

From IEEE INSTITUTE, Dec. 1987, p. 8:

CHIPS TOO UNRELIABLE FOR TRAINS, SAY ENGINEERS by Gadi Kaplan

"..This was one of the main conclusions at the Symposium on Microprocessors in Rail Transit, held in Pittsburgh on Sept. 14-16 by the Rail Systems Center of Carnegie-Mellon University's Mellon Institute. ...

Technical experts agree that microprocessor-based systems are more flexible in operation and much better at monitoring and fault diagnosis than the relay-based systems they typically replace. ...

Symposium participants expressed concern, however, about the probablity of failure of the microprocessor in an unsafe way as a result of inadequate verification of its software. A case in point was the failure, in February 1986, of a four-car train operated by the Washington Metropolitan Area Transit Authority (WMATA) to stop at a red signal. ... "The failure could not be replicated with the same cars at the same location under any condition with .. prolonged field and laboratory testing," (a WMATA official) reported...

However, a more postive view was expressed by panelists from ... suppliers of microprocessor-based systems for rail transport. These panelists said they were confident their software, which required years to develop, at extensive costs, was verifiable and reliable."

(End of excerpts from IEEE INSTITUTE)

- Jonathan Jacky

Addressable CATV systems

<ihnp4!ihuxv!tedk@ucbvax.Berkeley.EDU>
Wed, 25 Nov 87 07:39:33 PST

In my town, Oak Park, we have CATV provided by Cablevision of Oak Park. The CATV control boxes have a serial number which is recorded (and phoned in to the computer center) by the installer.

The digital signal broadcasted from the computer center (within the cable company) provides the boxes with the date and time. Niffy feature, localized time base for all devices. I have a button on my box for "display time" which is displayed at the top of my screen.

But most importantly the digital signal transmits an individually addressed (packet?) for each customer that provides a "matrix" of what each channel on the box vectors to from the cable. I have noticed that the order of the channels on the cable (itself) are different than what you see when you get with the CATV box. The "Un-Authorized" channels, such as Playboy and HBO, are _replaced_ with local cable guide (rather than the scambled signal and sound). The CATV box stores the matrix even if un-plugged from power. When the installer plugged in the box for the first time, all the channels where un-authorized.

When I call the cable company for a "pay-per-view", they update the matrix in my box to allow me to watch the program. The Matrix software in the box might even have "HOW LONG" information in it.

Now, How do I get the localized time base to keep my Microware oven clock on time ????? :-)

Ted G. Kekatos, AT&T Bell Laboratories, Indian Hill South, IX-1F-460
Naperville & Wheaton Roads - Naperville, Illinois. 60566 USA
backbone!ihnp4!ihuxv!tedk

A new legal first in Britain...

Gligor Tashkovich <gligor%lerouf.DEC@decwrl.dec.com>
25 Nov 87 20:15

I heard somewhere that Britain is experiencing a new legal first:

Apparently, a computer consultant is on trial there and is charged with criminal damage by planting "logic bombs" in his clients' software.

Does anyone else have more information?

---

the rm * controversy in unix.wizards

Charles Shub <cdash@boulder.Colorado.EDU>
Wed, 25 Nov 87 09:54:27 MST

Yesterday, I got bit by rm [REMOVE]. I was remotely logged in to a system over a network and had created a bunch of temp files. to delete them, I naturally typed in "rm t*" only the %$*#&^#@ network managed to drop the "t" and you all know what happened then. It wasn't too bad because with the

archiving we do it was only 2 hours to get them back. Of course yesterday's changes got lost and had to be redone. The point is that there are two things a command interface could do:
1) protect us from our own stupidity (I'm not convinced it should),
2) protect us from "extended system" errors like dropping a character,
but I'm not sure how you separate the two.

cdash aka cdash@boulder.colorado.edu aka ...hao!boulder!cdash
aka ...nbires!boulder!cdash aka (303) 593-3492

Search RISKS using swish-e

THE RISKS DIGEST

Forum on Risks to the Public in Computers and Related Systems

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

Volume 5: Issue 66

Friday, 27 November 1987

Contents

Mariner I

Eric Roberts <roberts@src.DEC.COM>
Wed, 25 Nov 87 18:33:14 pst

When Steve Berlin and I were writing the chapter on SDI for the new CPSR book _Computers in Battle_ (Boston: Harcourt Brace Jovanovich, 1987), I tried to track down a more complete reference to the Mariner I story. The theory that this was due to the substitution of a period for a comma in a FORTRAN DO statement seems to stem initially from the following quote from G.J.Meyers, _Software Reliability: Principles and Practice_ (New York: John Wiley, 1976):

> In a FORTRAN program controlling the United States' first mission to Venus, a programmer coded a DO statement in a form similar to the following:
>
> DO 3 I = 1.3P
>
> The mistake he made was coding a period instead of a comma.

> However, the compiler treated this as an acceptable
> assignment statement because FORTRAN has no reserved words,
> blanks are ignored, and variables do not have to be
> explicitly declared. Although the statement is obviously an
> invalid DO statement, the compiler interpreted it as setting
> a new variable DO3I equal to 1.3. This "trivial" error
> resulted in the failure of the mission. Of course, part of
> the responsibility for this billion-dollar error falls on
> the programmer and test personnel, but is not the design of
> the FORTRAN language also partially to blame?

Unfortunately, Meyers lists no references for this version of history. Some years ago, as part of the background work for the slide show _Reliability and Risk_, Steve Berlin had called to ask about sources for this story. Meyers could not remember an exact source.

Since this much tracing left me without a definitive source, I checked the _New York Times_ index and _Readers' Guide_ indices for 1962. The most informative article appeared in the _New York Times_ of Saturday, July 28--six days after the aborted launch:

> For Want of Hyphen
> Venus Rocket Is Lost
>
> By GLADWIN HILL
> Special to the New York Times
>
> LOS ANGELES, July 27--The omission of a hyphen in some mathematical data caused the $18,500,000 failure of a spacecraft launched toward Venus last Sunday, scientists disclosed today.
>
> The spacecraft, Mariner I, veered off course about four minutes after its launching from Cape Canaveral, Fla., and had to be blown up in the air.
>
> The error was discovered here this week in analytical conferences of scientists and engineers of the National Aeronautics and Space Administration, the Air Force and the California Institute of Technology Jet Propulsion Laboratory, manager of the project for N.A.S.A.
>
> Another launching will be attempted some time in August. Plans had been suspended pending discovery of what went wrong with the first firing.
>
> The hyphen, a spokesman for the laboratory explained, was a symbol that should have been fed into a computer, along with a mass of other coded mathematical instructions. The first phase of the rocket's flight was controlled by radio signals based on this computer's calculations.
>
> The rocket started out perfectly on course, it was stated. But the inadvertent omission of the hyphen from the computer's instructions caused the computer to transmit incorrect signals to the spacecraft....

The first paragraph makes it sound as if this might be a data entry error and not a coding error at all. Later paragraphs, however,

indicate that this was part of the "coded mathematical instructions."
Other references to the Mariner I failure appear in the letters section
of the _New York Times_ of August 2 (page 24) and in the August 6 issue
of _Newsweek_ (page 75) and seem to corroborate the view that this was a
programming error.

This account agrees with the recent report from Henry Spencer (RISKS-5.64)
who cites "Far Travellers" by Oran W. Nicks. On the whole, this explanation
seems to have more documentary evidence than the FORTRAN version of the story
presented by Meyers. The existence of other overstatements in his account
(in particular, $18,500,000 << $1,000,000,000) also reduces its credibility.

Of course, the FORTRAN version of the story has received widespread
distribution of late (it is, after all, a lovely story), including citations in

- Jim Horning, "Note on Program Reliability," _Software Engineering Notes_, 4:4, October 1979, p. 6.
- Peter Neumann, "Letter from the Editor," _Software Engineering Notes_, 8:5, October 1983, p. 4 (credited to David Smith of CMU, who heard it from his instructor in 1970 or 1971).
- H.S. Tropp, "Fortran Anecdotes," _Annals of the History of Computing_, 6:1, January 1984, p. 61.
- Peter Neumann, "Risks to the Public," _Software Engineering Notes_, 11:5, October 1986, p. 17.

However, unless there is more definitive evidence to support this, I
think it must be regarded as apocryphal.

My own solution in _Computers in Battle_ was to write:

> Shortly after its launch on July 22, 1962, the Mariner I
> Venus probe veered off course and had to be destroyed by
> mission control officials. The problem was later traced to
> a single character error in the controlling software.

This covers both explanations and seems to be on relatively safe ground.

/Eric

[Yes, but it bugs the question. PGN]

FORTRAN pitfalls (Re: RISKS-5.63)

Jim Duncan <jim@xanth.cs.odu.edu>
Thu, 26 Nov 87 13:40:20 EST

(Regarding the DO ... I=1.3 problem:)

I too have heard this `story' many times, and each time the space vehicle took
on a new name, and it was on its way to a different planet or mission. The
text I am reading for a course in principles of programming languages is the
first place I have seen this incident documented. The author is discussing
the design of syntactic structures in FORTRAN and the unfortunate effects of

adopting a lexical convention that caused blanks to be ignored everywhere:

"In FORTRAN, the statement

DIMENSION IN DATA (10000), RESULT (8000)

is exactly equivalent to

DIMENSIONINDATA(10000),RESULT(8000)

and, for that matter,

D I M E N S I O N IN DATA (10000), RESULT (8000)

While this may seem to be a harmless convenience, in fact it can cause serious problems for both compilers and human readers. Consider this legal FORTRAN statement:

DO 20 I = 1.100

which looks remarkably like the DO-statement:

DO 20 I = 1,100

In fact, it is an assignment statement of the number 1.100 to a variable called `DO20I', which we can see by rearranging the blanks:

DO20I = 1.100

You will probably say that no programmer would ever call a variable `DO20I', and that is correct. But suppose the programmer _intended_ to type the DO-statement above but accidentally types a period instead of a comma (they are next to each other on the keyboard). The statement will have been transformed into an assignment to `DO20I'. The programmer will probably not notice the error because `,' and `.' look so much alike. In fact, there will be no clue that an error has been made because, conveniently, the variable `DO20I' will be automatically declared. If you think things like this can't happen, you will be surprised to learn that an American Viking Venus probe was lost because of precisely this error."

The above is from Bruce J. MacLennan, _Principles_of_Programming_Languages_ (second edition), CBS College Publishing, 1987, pp. 89-90. Mr. MacLennan goes on to elaborate on the principles of good language design violated by FORTRAN, such as Defense in Depth.

To add my two-cents worth: When I first heard the Viking story, I inferred that the offending DO-statement was in the code which either positioned the navigational motors, or did the navigation calculations. I was told that the launch went perfectly and the probe reached the desired earth orbit. When the probe fired its motors to leave earth orbit, however, it supposedly rolled over on its back, fired in the wrong direction, and promptly _disappeared_ from all tracking systems. No one knows where the hell it went....

Jim Duncan, Computer Science Dept, Old Dominion Univ, Norfolk VA 23529-0162

(804)440-3915 INET: jim@xanth.cs.odu.edu UUCP: ...!sun!xanth!jim

PIN verification

<MAKELA_O%FINJYU.bitnet@csl.sri.com>
Thu, 26 Nov 87 13:11 O

In RISKS 5.61, John Pershing <PERSHNG@ibm.com> writes:
>I cannot speak for *all* ATM and POS systems, but the major banks
>generally know what they are doing with respect to PIN security. The PIN
>number is *not* stored on your ATM card -- it is stored in your bank's
>database and, possibly, in one or more interbank clearinghouses. This
>makes it possible to have your PIN changed without getting the card
>re-magnetized (assuming your bank has it's act together). Note that your
>account number probably isn't even written on the card -- only a number
>that identifies that particular card. [...]
>John A. Pershing Jr., IBM, Yorktown Heights

Well, it *would* seem that the Finnish banks use a different system. Perhaps I should first describe the most common types of plastics we have here:

* the autoteller cards, that can only be used in ATM's
* the "Bank Cards", that work at ATM's and can be used for buying stuff; using them is legally the same as writing out a cheque for the same amount
* the VISA-combocard, that is a combined ATM/Bank Card/VISA-card; when you use them for buying stuff you have to tell what you want it to be used as

All the abovementioned cards DO have the attached account number on them. It is possible also to have SEVERAL accounts on them, but I'm not sure how this is accomplished. This option is only offered by one bank, so it might be just their hack.

Follows a paragraph from the official guide to implementing off-line POS terminals using magnetic card identification:

> PIN-verification is done by the Security Unit, which is connected to the POS terminal, according to the the PVV-number, which is read off the magnetic stripe of the card. The requirements for PIN-verification are given separately in "POS terminal security standards". Written requests for the distribution of these standards may be sent to AIP-security Chief Lars Anrkil, SKOP (Kilo), PL 400, 00101 HELSINKI.

[SKOP is a big Finnish banking group, more or less a "collection of competing fiefdoms", as David G. Grubbs <dgg@dandelion.CI.COM> put it in RISKS 5.61; it would seem that the Finnish Banking Association has given them the job of maintaining and distributing these security standards.]

Here's a few arguments against the systems working by being on-line to the bank computer or some other similar system:

* the guide was for OFF-LINE POS terminals.

* the same PIN-numbers are used internationally, in VISA-card -based ATM-type machines, where you use your VISA-combocard to get money that will be billed in your next VISA bill. I have difficulties believing that even in this information age they would maintain a computer link from all over the world to remote Finland :-)
* I have several times went to an ATM that is used by several banks in co-operation, inserted my card, typed in my PIN and received a message saying "Your bank's computer is down". The PIN was verified BEFORE the ATM tried to contact my bank's computer.
* I have asked several times if it is possible to change my card's PIN number (just to know if it is possible), and have always received a reply stating "no, it's not possible, it's derived from your card number". This is very weak, since bank people generally aren't that good on technical aspects...

I think these taken together are pretty strong indications that the PIN verification CAN be done off-line, at least for the Finnish standard of cards.

I dearly do hope that security in these systems is not maintained by secrecy ONLY! However, I have had the company I work in part-time order the set of security standards, so as soon as we get them, I'll let you people know more...

Otto J. Makela, U of Jyvaskyla
Mail: Kauppakatu 1 B 18, SF-40100 Jyvaskyla, Finland
Phone: +358 41 613 847
BBS: +358 41 211 562 (V.22bis/V.22/Bell 212A/V.21)
BitNet: MAKELA_OTTO_@FINJYU.bitnet

Sudden acceleration revisited

Leslie Burkholder <lb0q+%andrew.cmu.edu@ROME.UCI.EDU>
Thu, 26 Nov 87 13:15:59 -0500 (EST)

Honda motor company has offered replacements for the chip controlling acceleration in the 88 Civic. Some people have complained of problems with this chip in their Civics.

Re: CB radio and power (RISKS-5.64)

"Maj. Doug Hardie" <Hardie@DOCKMASTER.ARPA>
Wed, 25 Nov 87 11:44 EST

[For the record. Truth-in-harmonics department.]

> The second harmonic of 26-27 Mhz signals rounds out to 104-108 Mhz,
> or the upper half of commercial FM radio. [Jeffrey R Kell. RISKS-5.64]

According to my understanding of the new-new-math (I am a product of the new math), that would have to be the fourth harmonic.

-- Doug

[I hope no one pleads the fifth. 130-135 would sound

suspiciously like late Beethoven String Quartets.
Gesunta-heit. PGN]

An earlier train crash -- Farnley Junction

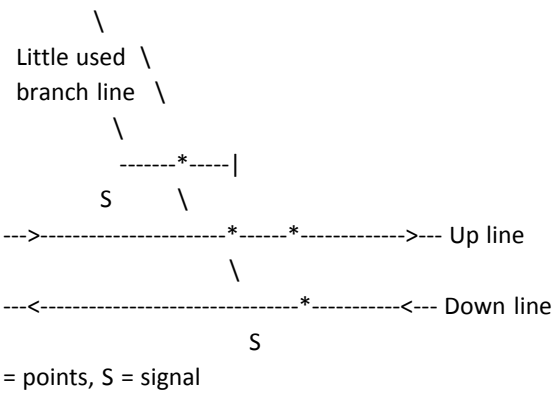
"Clive D.W. Feather" <mcvax!root.co.uk!cdwf@uunet.UU.NET>
27 Nov 87 16:48:37 GMT

Not quite computers, but after the item in RISKS-5.64 about the Swedish train crash, readers might find this interesting.

Summary of official report on accident at Farnley Junction (Yorkshire) in 1977, on British Railways.

Farnley Junction is a few miles from Leeds Signal Box, and is remotely controlled from there. All safety interlocking logic is in the signal box itself (all signalling in this area is carried out by 12V relay logic). The distance is such that an intermediate repeater unit repeats all relay signals between the junction and the box.

The physical layout is as follows:



Normal logic, e.g., for signals, is binary, but the controls and position detection of the up-to-down-line crossover happened to be trinary (line A positive = straight ahead, line B positive = cross over, neither positive = no command / not correctly set).

On the day in question, a fault at the repeater unit was causing problems. Both signals were set to Danger by the signalman, and an engineering team then changed the rectifier in the power supply at the repeater unit.

The loss of power caused the main signalling logic to believe the crossover was not correctly set (no repeat of the detection), and so it set the control lines to drive the crossover back to the stright ahead position (this will stay driven until the detection is correct - meantime, the signals are locked at Danger).

Trains came to a halt at both signals.

The engineers restored power to the repeater, but had wired in the rectifier

the wrong way round. This had the effect of reversing the polarity of voltages repeated - not important for binary signals.The crossover took the incoming voltage as a command to move to the "crossover" position, and did so. The detection mechanism correctly reported "crossover" - this was reversed at the repeater, and the main signalling logic (correctly) took the incoming signal to mean that the points were locked in the "straight ahead" position.

The signalman now set both signals to Proceed, and the signalling logic allowed him to do so. The train on the Up line started off immediately (the other driver was trying to figure out why the points were set the wrong way !), traversed the crossover, and collided with the train on the Down line, killing two people.

I know this isn't computing, but there's a lesson in it, even so.

> [Don't lessen the lesson by thinking this isn't computing.
> Circuitry, programs, algorithms, and people have much in common. PGN]

Search RISKS using swish-e

THE RISKS DIGEST

Forum on Risks to the Public in Computers and Related Systems

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

Volume 5: Issue 67

Monday, 30 November 1987

Contents

Aging air traffic computer fails again

Rodney Hoffman <Hoffman.es@Xerox.COM>
28 Nov 87 11:31:06 PST (Saturday)

In RISKS 4.48 (18 Feb. 87), I related how flights throughout Southern California were delayed due to the failure of the "9020" air traffic computer at the L.A. Air Route Traffic Control Center. Since the 9020 failed 12 times during the last six months of 1986, this story violates the masthead guidelines about being nonrepetitious. However, in the Feb. outage, it was reported that

the 18-year-old system was "expected to be replaced later this year" [1987].

Following Murphy's Law, not only has the replacement not yet happened, but the system's latest failure was on one of the busiest travel days of the year -- the Wednesday before Thanksgiving, when the passenger load was 40% more than on a normal weekday. Additionally, a bomb scare forced an emergency landing of one plane, further fouling flight schedules.

The computer failure, attributed by the L.A. Times to a "software problem" in the "massive IBM computer ... that controls high-altitude air traffic for much of California, Arizona, Nevada, and Utah" lasted 4.5 hours, delayed over 140 flights from Southern California airports for 30 minutes to two hours. The L.A. Air Route Traffic Control Center is one of 20 such FAA regional facilities in the U.S.

Officials stress that the computer failure posed no danger to airline safety. Instead, it forced controllers to shift to a slower backup computer and "to carry printed information by hand, limiting the volum of traffic they can handle." The news accounts made no mention this time of a date for installation of a replacement computer system.

-- Rodney Hoffman

Air traffic computer failure?

Alan Wexelblat <wex@MCC.COM>
Fri, 27 Nov 87 12:21:03 CST

COMPUTER BREAKDOWN SLOWS FLIGHTS IN WEST

Los Angeles(AP) - A five-hour air traffic control computer failure Wednesday [the day before Thanksgiving] stalled the holiday weekend getaway for thousands of Californians. The computer broke down at about 5:30AM and wasn't back in operation until about 10:30AM, said a spokesman for the Federal Aviation Administration. The computer in Palmdale, 60 miles north of downtown LA, routes air traffic for Southern California and sections of Nevada and Arizona. The cause of the failure was not immediately determined. The failure forced controllers to shift to a backup system that provides less information and the slowed operations, but no safety problems were encountered, the FAA spokesman said.

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

[At San Francisco Airport they were advertising the worst day of the year, and delays did propagate... PGN]

Computer Virus

Jeffrey James Bryan Carpenter <JJC%Vms.Cis.Pittsburgh.Edu@VB.CC.CMU.EDU>
Wed, 25 Nov 87 11:15 EDT

From: IN%"MD4F@CMUCCVMA" "User Services List (ADVISE-L)" 23-NOV-1987 09:33

To: Jeff Carpenter <256521@vms.cis.pittsburgh.edu>
Subj: Virus warning!
Date: Mon, 23 Nov 87 08:05:57 EST
From: "Kenneth R. van Wyk" <@vms.cis.pittsburgh.edu:LUKEN@LEHIIBM1.BITNET>

Last week, some of our student consultants discovered a virus program that's been spreading rapidly throughout Lehigh University. I thought I'd take a few minutes and warn as many of you as possible about this program since it has the chance of spreading much farther than just our University. We have no idea where the virus started, but some users have told me that other universities have recently had similar probems.

The virus: the virus itself is contained in the stack space of COMMAND.COM. When a pc is booted from an infected disk, all a user need do to spread the virus is to access another disk via TYPE, COPY, DIR, etc. If the other disk contains COMMAND.COM, the virus code is copied to the other disk. Then, a counter is incremented on the parent. When this counter reaches a value of 4, any and every disk in the PC is erased thoroughly. The boot tracks are nulled, as are the FAT tables, etc. All Norton's horses couldn't put it back together again... :-) This affects both floppy and hard disks. Meanwhile, the four children that were created go on to tell four friends, and then they tell four friends, and so on, and so on.

Detection: while this virus appears to be very well written, the author did leave behind a couple footprints. First, the write date of the command.com changes. Second, if there's a write protect tab on an uninfected disk, you will get a WRITE PROTECT ERROR... So, boot up from a suspected virus'd disk and access a write protected disk - if an error comes up, then you're sure. Note that the length of command.com does not get altered.

I urge anyone who comes in contact with publicly accessible (sp?) disks to periodically check their own disks. Also, exercise safe computing - always wear a write protect tab. :-)

This is not a joke. A large percentage of our public site disks has been gonged by this virus in the last couple days.

Kenneth R. van Wyk, User Services Senior Consultant,
Lehigh University Computing Center (215)-758-4988
<LUKEN@LEHIIBM1.BITNET> <LUKEN@VAX1.CC.LEHIGH.EDU>

Fiber optic tap

<portal!cup.portal!Kenneth_R_Jongsma@Sun.COM>
Sat Nov 28 18:09:48 1987

Up until now, one of the prime advantages of fiber optic cable (aside from its capacity) has been its perceived resistance to being tapped by unauthorized parties. The Nov. 16th issue of EE Times had an interesting article that may change those perceptions.

EE Times reports that Plessey has developed a non-intrusive way of tapping fiber optic cable. The article states that Plessey's design concept has been tested with both high-speed digital as well as television signals. They don't go into details, but do say that the device clamps over an existing cable and bends it slightly. The small amount of light that is released from the cable can be detected and amplified.

They do acknowledge the fact that this causes problems for system security, but feel that the advantages (primarily in making it cheaper to use fiber as a cable tv medium) outweigh any disadvantages.

I find the implications of this development rather startling. They don't give a price for the device, but given that it is intended to be used as a cable tv line splitter, it can't be out of the reach of any individual.

A new and possibly risky use for computer chips

John Saponara <saponara@tcgould.tn.cornell.edu>
Mon, 30 Nov 87 12:19:28 EST

An interesting use of computer chips was mentioned in "The Christian Science Monitor" in the November 13, 1987 issue, in an article titled "Showdown takes shape over plastic weapons":

> Plastic firearms - now being developed for the United States Army by Red Eye Arms Inc. - are a bone of contention between antigun organizations and the National Rifle Association (NRA).

[The article goes on to tell of the opponents, then continues:]

> "One of the worst nightmares in our fight against terrorism is the possibility that airline hijackers could carry plastic guns aboard aircraft without detection," says Senator Metzenbaum. "In order to prevent this frightening scenario, we need to act now."
>
> But David Conover of the NRA says: "Firearms constructed completely out of plastic don't exist now." He argues that a ban on this "future" technology does not address the real problem of faulty airport security at the root of terrorist activity.
>
> John Floren, president of Red Eye Arms - which holds the only patent to produce such weapons - says the prototype his firm is developing for the Army would be entirely plastic but would have computer chips implanted to make possible detection of make, model, and serial number from 15 feet away.

[The article goes on to describe the uses of plastic arms and various legislation concerned with them.]

The idea of adding chips to plastic guns, then selling chip detectors to all the airport security checkpoints, seems lucrative but does not strike me as the most sensible approach to the problem. I have not heard of the use of computer chips as a detection scheme before. How foolproof is such a scheme? If I

stopped sending current to the chip, would the gun then not fire? Could I reprogram these chips to have false ID's from other guns, or to not transmit? Considering the problems the cellular phone companies have had with reprogrammed phone chips, there seem to be real possibilities of circumventing such measures. Does anyone know of any similar detection systems in use at present, and how secure they are?

Eric Haines

Selling Science [a review]

Peter J. Denning <pjd@riacs.edu>
Mon, 30 Nov 87 12:13:26 pst

Many RISKS readers have struggled with the question of generating a rational public debate when complex technical issues are involved. What follows is a review of an interesting little book chock full of insights into how science journalism works and interacts with the scientific research community. The author's comments on treatment of risks in the media are particularly interesting. I recommend the book highly. (pjd)

Selling Science, Dorothy Nelkin, W. H. Freeman, 1987, 224pp.
A review by Peter J. Denning

Have you ever wondered about the apparent contradiction between hyperactive science journalism and extensive scientific illiteracy? Between the promotion of technology as the key to progress in society and the growing fear of technology? Between the demand for sophisticated science-based medicine and the widely supported objections to animal experiments? Between the rationality of science and expectations of ``magic bullets'' and ``miracle cures''? Have you ever wondered whether you will be misrepresented if you talk to a journalist, whether having your research discussed in Newsweek is essential to your continued funding, or whether ``popularizers'' like Carl Sagan are advancing science? If you have, you are not alone.

These questions touch on fundamental issues in science, technology, and the press. Dorothy Nelkin has faced them head on in this fascinating book. With clarity and painstaking documentation she identifies four main characteristics of science journalism. First, most articles are high in imagery and metaphor, and low in technical content. Many of the images show science as arcane, esoteric, beyond normal understanding, authorative, trustworthy, pure, neutral, and the ultimate source of rationality and basic truth. High technology is touted as a quick fix to many problems and is the source of much disillusionment when it fails. On debates of great controversy, such as ozone, artificial sweeteners, or dioxin, or strategic defense, little technical information is given; instead equal time is given all ``sides'' no matter how irrational they might be from an objective standpoint. Second, much of science is portrayed as a series of dramatic events, rather than the slow, backtracking, plodding process it really is. Third, there is a strong emphasis on competition -- e.g., the ``race'' for breakthroughs, the obsessive 90-hour workweeks of Nobel laureates, or the ``technology war'' between the United States and Japan. Fourth, scientists

have been actively involved in the press; far from being neutral sources, they have sought favorable coverage of their projects. Many institutions have active media programs that have successfully put the most favorable information out for public consumption, professional societies have advanced proposals to control the flow of information to the press, and some journals by policy refuse to publish any finding that has been ``scooped'' in the public press. In the midst of this, scientists have ambivalent attitudes toward the press, at some times seeking it out, at others criticizing it.

These trends emerge from Nelkin's careful analysis of a large number of scientifc articles published over many years, and they correlate well with one's own experience. But the real contribution of the book lies in its careful, and highly successful attempt to understand the frames of reference -- the mindsets -- of scientists and of journalists. Nelkin accurately describes the style of scientific research, the norms of objectivity (especially peer review and reproducibility of results), the professional ideals, the role of technical jargon, and the rules of evidence widely used in science -- in short, the unspoken culture in which all scientists operate. She similarly describes the culture of journalism, including basic reporting, editorial contraints, audience assumptions, economic pressures, avoidance of complexity, and vulnerability to sources. From this it becomes easy to appreciate the sources of misunderstandings between scientists and journalists. When a scientist says there is no (statistically significant) evidence of a correlation between power-plant radiation and cancer, a journalist who knows of a few cases of radiation-induced cancer may ``hear'' a coverup; when a scientist says a new drug produced an improvement in a few AIDS patients, a journalist may ``hear'' that a cure is imminent. When a journalist asks probing questions about risks of technology, a scientist may ``hear'' that the journalist is trying to make the evidence fit his own hidden agenda; when a journalist omits important methodological details about an experiment, a scientist may ``hear'' an attempt to oversell a finding to a gullible public.

Nelkin praises efforts to increase mutual cultural understanding between scientists and journalists, such as formal science training for science journalists, the Council for Advancement of Science Writers, and the Media Resource Service of the Scientists Institute for Public Information. Although the tension can be softened, she says, the two cultures are inherently different and the tension cannot be wholly eliminated. Scientists and journalists will have to come to terms with an uneasy, occasionally adversarial relationship.

Risks to computerised traffic control signs

Peter McMahon <munnari!uqcspe.cs.uq.oz.au!pete@uunet.UU.NET>
Mon, 30 Nov 87 13:07:50 est

Quoted from "Computing Australia", without permission. [23 Nov 87]

"Computer-run signs over Canterbury Road in Melbourne's eastern suburbs suggested a speed of 75 km/h - in a 60 km/h zone - for a clear run through traffic lights.

Despite the anger of police the mix-up was not solved for three days.

The 26 electronic signs are part of a new information system devised by the Road Traffic Authority (RTA) [...]

[An obviously upset!] Chief Superintendent Frank Green of the Victorian Police traffic department said: "If these mongrel machines are telling people to breach the bloody law we'll have to tell the RTA to take its computer and shove it."

RTA and Mach Systems officials denied any bungled programming and said that only two signs were malfunctioning."

Peter McMahon, Computer Science, University of Queensland, Australia
pete@uqcspe.cs.uq.oz.au

Risks in Energy Management Systems

<Anon @ uk academic establishment>
26 Nov 87 16:07:33 GMT (Thursday)

A while back someone asked about risks in Energy Management Systems; well, here's one that I know of (even though it isn't related to computer rooms, unlike the original discussion)....

Some time ago I spent about nine months working for a company which produces and sells a computer controlled distributed energy management system. It consists of outstations (which can work stand-alone) and a central operators station. The centre was running circa 10000 lines of uncommented, undocumented spaghetti BASIC which had evolved over a period of years in the care of a couple of self-taught programmers. The outstations contained a few thousand lines of commented but undocumented assembler. Communication was by reading & writing of memory in the outstation using explicit memory addresses embedded in the centre software.

[My job was supposed to be to help them do a complete redesign & reimplementation, but that was 'temporarily' shelved when the Managing Director realised what it would cost (amongst other reasons)]

The standard mechanism for fixing a bug involved someone trying to replicate it, hacking a fix into a copy of the user's version of the program & then sending it back to them. No version control, no replication of fixes across the user base etc. Testing involved installation on-site & waiting a day or two to see if things broke. The only in-house tests were done by running new software in the outstation that controlled the company HQ : I've seen clients sitting in our reception area in hat & coats on a Monday morning (waiting to see someone) because the heating hadn't switched itself on (there was a warm-up period so manual over-rides at 8am didn't have much effect until after 10) and as a result in-house tests were strongly discouraged!

Not surprisingly, crashes were common - especially of the 'centre' - which

was embarrassing since the system - originally designed for control of heating plant in schools & factory complexes (eg one centre for an education authority, one outstation per school) - was also being used as heating control for communal housing projects.

However, the worst incident was in fact hardware related. UK mains voltage is 240V +/- a maximum percentage. The outstations contained a transformer which would drop out (powering down the system) if the voltage dropped more then a couple of volts below the (supposedly) absolute minimum, it would only trip in again at nearly 240V (quite a lot of volts above this minimum). Last winter was quite severe over here and there was some strain on the electricity supply system so it ran at near minimum for extended periods (several hours at a time) with occasional glitches down to the absolute minimum and (we suspect) sometimes slightly lower. Now, when an outstation stopped it halted all of the pumps, boilers etc that it controlled; ie no heating was provided.

Because of the way power was supplied to an outstation in a communal housing project it was receiving a couple of volts below the actual mains voltage and one evening it tripped out. It didn't trip in again until a LOT of hours later, by which time all of the housing involved had got very cold. The accommodation included some sheltered housing for elderly people one of whom ended up requiring hospital treatment for hypothermia. Fortunately for the company nobody sued and the woman involved recovered (remember that hospital treatment over here is free so there were no medical bills involved).

This sort of problem was far from unique, it's just that the people who are buying these systems often don't realise the potential dangers and some manufacturers are so busy trying to grab a share of the market that they rush bad &/or untested products to the buyers.

Search RISKS using swish-e

THE RISKS DIGEST

Forum on Risks to the Public in Computers and Related Systems

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

Volume 5: Issue 68

Tuesday, 1 December 1987

Contents

Logic Bomb

Brian Randell <br%kelpie.newcastle.ac.uk@NSS.Cs.Ucl.AC.UK>
Fri, 27 Nov 87 10:57:34 GMT

Here, in response to Gligor Taskovich's request in RISKS DIGEST 5.65, is an article on the trial here in the UK relating to a "logic bomb". It comes from Computer Weekly, November 26, p. 3, and is quoted here in full. (br)

MAN CHARGED WITH PLANTING TIME BOMB

Criminal damage charges have been brought against a computing specialist who allegedly doctored a customer's software so it would give his firm a contract to put things right. James McMahon, 32, from Watford denies four charges of criminal damage and one attempt at criminal damage to discs and systems belonging to Pandair Freight, obtaining over (pounds)1,000 from Pandair by deception for his company, Wendmist, and attempting to obtain (pounds)372.

In January 1986 Pandair's system in Heston, Middlesex, running on a DEC computer, broke down. Prosecutor David Radcliffe told the court that the problem was caused by a time bomb, inserted earlier. The 1985 version would still work but after McMahon spent time on it things got worse, Radcliffe said. McMahon arranged to work on the faults on returning from holiday. While he was away a Pandair programmer did some tests and found a section of unauthorised code. "He found the time bomb and defused it," Radcliffe said. The programmer then looked at a similar system at Pandair's Birmingham office. Here he found a time bomb which would have erased the computer's memory.

Radcliffe suggested McMahon had acted out of revenge, because he had just failed to win a (pounds)50,000 contract to update Pandair's system at Maidenhead. Pandair says the system problems cost it (pounds)15,000.

This is believed to be only the second case of alleged criminal damage of its kind. The first, last year, followed a farewell prank by a Dixons employee who tried to get the company's mainframe to display "goodbye folks" whenever his leaving date was entered in staff records. he was conditionally charged and orderd to pay Dixons (pounds)1,000.

John Kavanagh

UK Logic Bomb Case

"ZZASSGL" <ZZASSGL@CMS.UMRCC.AC.UK>
Mon, 30 Nov 87 12:35:49 GMT

[This contribution included TWO news reports, including excerpts from the article noted above. It also commented thereupon. PGN]

Both reports are somewhat confusing about the actual details, but the basic facts seem simple. McMahon did some work on the system, was expecting to get a contract for more, but didn't. Shortly after the system had problems and when Pandair programmer investigated he found the ''bombs''. As the case is still proceeding it is not possible to connect these two facts.

I remember reading an earlier report (I can't find it now) about the problems that were expected because the jury would have to understand the background and jargon before being able to decide the case. They were all provided with a glossary for the technical terms to be used and also given a one day introduction to computers and DEC systems.

Re: hyphens & Mariner I

Jerome H. Saltzer <Saltzer@ATHENA.MIT.EDU>
Sun, 29 Nov 87 01:30:11 EST

As long as people are still searching for the real story, here is another possible clue, based on yet another third-hand rumor: Back in 1962, when Mariner I failed, the story that quickly circulated around M.I.T. was that a minus sign had been miscoded as a hyphen. You see, the keypunches in those

days had two different keys with similar-looking graphics, one interpreted as a minus sign, the other as a hyphen. The first Fortran compiler accepted only the minus sign for the subtraction operator. At one point in the evolution of that compiler a (fatal!) diagnostic was added to alert you that you had used the "wrong minus sign," leading to snide comments along the line of "if you're so smart, why don't you fix it?" and a standard test of skill was to figure out how to patch the Fortran compiler to accept a hyphen as an alternate minus sign. When a hyphen appeared in data, the result depended on the software that was trying to interpret it; some programs accepted it as an alternate minus sign, other programs ignored hyphens (effectively reversing the intended sign), and still other programs blew out with a bad data diagnostic. Given that kind of confusion every day in the keypunch room, when the rumor about Mariner I came through it sounded very plausible.

Whether or not Mariner I was a victim of hyphen/minus-sign confusion, the keypunches of the late 50's carry a cautionary tale for RISKS readers.

Jerry Saltzer
[Hyphen the Terrible? PGN]

<ucbcad!ames.UUCP!uw-beaver!ssc-vax!wanttaja@ucbvax.Berkeley.EDU>
Fri, 27 Nov 87 00:25:40 pst

(Ronald J Wanttaja)
To: uw-beaver!KL.SRI.COM!RISKS
Subject: Re: Mariner, and dropped code

I was in a NORAD satellite operations unit for four years, and "I was there" during several times when erroneous attack warnings were generated.

One sticks in my mind... it wasn't caused by a missing hyphen, or replacing a period with a comma, but by an INCORRECT VALUE OF *PI*! I dearly wish I had bothered to find out what the value had been, but, considering the circumstances of the error, it probably was in one of the later decimal places.

The system worked as advertised and the attack warning was quickly cancelled.

[This and Jerry Saltzer's contributions are just two of many that have been backlogged. More is coming... PGN]

Minuteman and Falling Trucks

Joe Dellinger <joe@hanauma.STANFORD.EDU>
Mon, 30 Nov 87 02:46:45 pst

I was curious to find out how often incidents such as the "truck parked on the missile silo door" one mentioned here really occur, and how stupid this response really was. As it happens, my brother was until a few years ago the commander in charge of missiles at a Missouri base.

While the answers to some of my questions were classified, here's what he said (as I understood it):

False "launch in progress" status warnings aren't that rare. He saw about one per year at his base. There is a definite set of procedures to perform when this happens. Parking a truck on top of the silo door such that it will fall in on top of the missile if the door opens is one of them. The people that did this were doing the officially approved thing! The truck is to be parked such that one set of wheels is on terra firma and the other set is on the silo door. The truck is to be left in neutral with the parking brake off. The door itself is designed to open despite any debris on it, and there is a lip of sorts on the door to keep the debris from falling off the door and onto the missile. However, this lip can't handle more than a few inches worth of debris. The truck, properly parked, has no way of riding the door and will fall something like several hundred feet onto the missile. The damage thus inflicted should serve to "keep the missile in the hole". Worst possible outcome (unlikely to happen) is that the missile detonates its nuclear warhead in the hole, resulting in a quarter-mile wide crater and some local contamination.

The silo door can be opened and closed with a hand crank, but even if you know all the required access codes (which no one person does) you don't have time to get to the crank before the security people have time to get to you.

I've seen a field where missiles are kept. Looked just like any other farmer's field in the area to me, except that the "keep out" signs were especially intimidating and there were no cows in it. I was amazed to discover that the missile field was right next to a state highway!

- joe@hanauma.stanford.edu

Re: Fiber optic tap

Mike Muuss <mike@BRL.ARPA>
Tue, 1 Dec 87 16:20:52 EST

Your message is neither surprising, nor is it "news". The device used by AT&T to splice cables "in the field" has used this principle for years. The device is suitcase-sized, rugged, portable, and inexpensive (< $100k). It injects a signal on one side of the splice, monitors the signal on the other side of the splice, and mechanically optimizes for the maximum transmission through the splice, then heat-welds the two fibers. The signal injection and recovery is non-intrusive and non-damaging, and very very easy.

Dr. Steve Wolff (now of NSF, formerly of BRL) jointly holds a patent for a spatial light modulation technique that renders this type of tapping useless. However, to my knowledge, there are no production modulators that embody this technique.

In summary, only physical security and encryption provide acceptable security for important transmissions.

-Mike Muuss, Advanced Computer Systems Team, BRL

Re: Garage Door Openers

<mnetor!utzoo!henry@uunet.UU.NET>
Fri, 27 Nov 87 12:33:09 EST

> An Army spokesperson denies that the Army is radiating anything that
> would lock up these receivers.

What they may actually have said, or meant to say, is that they are not radiating anything that *should* lock up those receivers. Much consumer electronic equipment is cheaply (in both senses of the word) designed and is very vulnerable to interference from signals that theoretically it should ignore. Things like ham-radio transmissions interfering with TV reception are often the fault of the TV set, not the perfectly-legal-and-proper radio transmitter. The problem actually is not restricted to consumer equipment; things like police radars are often rather unselective as well.

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

---

Dutch Database Privacy Laws

Robert Stanley <roberts%cognos%math.waterloo.edu@RELAY.CS.NET>
27 Nov 87 19:50:18 GMT

The following is an extract from a recent posting to comp.society.futures. This is a very advanced approach to the problem, and it would be extremely interesting to have more detail on the law in question. The issue of implementation is not totally resolved, however. I assume that the law requires each GOAL to be registered, and that some agency is empowered to audit and/or investigate (the latter only in the event of reasonable suspicion of misuse). But how do we prevent the meta-database of database GOALS from being misused - quis custodiet ipsos custodes remains true as the day it was written.

| From: FRUIN@HLERUL5.BITNET.UUCP
| Newsgroups: comp.society.futures
| Subject: Filtering A Global Hypermedia Network
| Organization: The ARPA Internet
| Posted: Fri Nov 20 08:18:00 1987
|
| In Holland a new law will soon take effect regarding databases that store
| information about people. It's basic premise is that a database should have
| a GOAL, i.e. to send you your electricity bill or to keep track of your car's
| registration number. It is FORBIDDEN two match or combine any two databases
| that don't have the same goal. You can take anybody to court who does so
| anyway. This should make it very hard for corporations and government agencies
| to access any information about you.
|
| -- Thomas Fruin
|
| fruin@hlerul5.BITNET
| thomas@uvabick.UUCP

| 2:500/15 on FidoNet
|
| Leiden University, Netherlands

On a slightly different subject, I am becoming increasingly aware of a new computer-related problem which may yet develop into a full-blown risk. In our working environment we are pretty well established as workstation-per-user, and the technology of networking means that it is sometimes easier to relocate people rather than reconfigure electronic offices. We have a fair number of tools for which we have site licenses limiting us to x copies (x <= 5 for our group of 18 is typical). What we want is ability to run no more than 5 simultaneous copies at any of 18 workstations, what we have is software enabled on 5 specific workstations. Not only is this damnably awkward at times, but it can introduce a number of problems.

First of all, there is the classic problem of protected software. We use Sun/3 workstations, and the first engineering response to problems is swap out the processor board (our workstations are single-board). At this point we are in the identical position of the person who has irretrievably damaged their key-disk for a copy-protected micro product, because the workstation's serial number has changed. We have a company policy that pretty much says that no critical data will be dependent on a program for which we cannot generate replacement/alternate versions in case of emergency.

The second problem is when installation of software changes the workstation in subtle but important ways. When people shift workstations in order to access one of these restricted applications, the displaced owner can find him/herself misusing the (temporary) alternate environment. Once you have worked for a while on a configurable workstation, you rapidly forget how much of its behaviour is default, and how much is your customizing. Until, that is, you find yourself in an environment which appears almost the same, but behaves drastically differently in some key and unobvious fashion. Of course, there are ways round this, but the problem is a direct result of lazy or sloppy thinking on the part of the application vendor.

The vendor solution is to have a copy of their software on every workstation, but that is a totally unacceptable solution from the cost standpoint unless some massive price breaks are introduced. Interestingly, as standards such as X come into common implementation, we may end up remote-logging-in to a software server to which such tools are licensed, with X supplying the full interactive graphic windowing capability at the remote workstation. Back to the days of time-sharing a central computer!

R.A. Stanley Cognos Incorporated S-mail: P.O. Box 9707
Voice: (613) 738-1440 (Research: there are 2!) 3755 Riverside Drive
FAX: (613) 738-0002 Compuserve: 76174,3024 Ottawa, Ontario
uucp: decvax!utzoo!dciem!nrcaer!cognos!roberts CANADA K1G 3Z4

Report problems with the web pages to the maintainer

Search RISKS using swish-e

THE RISKS DIGEST

Forum on Risks to the Public in Computers and Related Systems

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

Volume 5: Issue 69

Friday, 4 December 1987

Contents

Can you sue an expert system?

<portal!cup.portal!Barry_A_Stevens@Sun.COM>
Thu Dec 3 21:34:16 1987

I am interested in the legal aspects of using expert systems.

Consider, and please comment on, this scenario.

* * * * * * * * * * *

A well-respected, well-established expert systems(ES) company constructs an expert financial advisory system. The firm employs the top ES applications specialists in the country. The system is constructed with help from the top domain experts in the financial services industry. It is exhaustively tested, including verification of rules, verification of reasoning, and further analyses to establish the system's overall value. All results are excellent, and the system is offered for sale.

Joe Smith is looking for a financial advisory system. He reads the sales literature, which lists names of experts whose advice was used when building the system. It lists the credentials of the people in the company who were the implementors. It lists names of satisfied users, and quotes comments that praise the product. Joe wavers, weakens, and buys the product.

"The product IS good,", Joe explains. "I got it up and running in less than an hour!" Joe spends the remainder of that evening entering his own personal financial data, answering questions asked by the ES, and anticipating the results.

By now, you know the outcome. On the Friday morning before Black Monday, the expert system tells Joe to "sell everything he has and go into the stock market." ESs can usually explain their actions, and Joe asks for an explanation. The ES replies "because ... it's only been going UP for the past five years and there are NO PROBLEMS IN SIGHT."

Joe loses big on Monday. Since he lives in California, (where there is one lawyer for every four households, or so it seems, and a motion asking that a lawsuit be declared frivolous is itself declared frivolous) he is going to sue someone. But who?

The company that implemented the system?

The domain experts that built their advice into the system?

The knowledge engineers who turned expertise into a system?

The distributor who sold an obviously defective product?

Will a warranty protect the parties involved? Probably not. If real damages are involved, people will file lawsuits anyway.

Can the domain experts hide behind the company? Probably not. The company will specifically want to use their names and reputations as the source of credibility for the product. The user's reaction could be, "There's the so-and-so who told me to go into the stock market."

Can the knowledge engineers be sued for faulty construction of a system? Why not, when people who build anything else badly can be sued?

How about the distributor -- after all, he ultimately took money from

the customer and gave him the product.

* * * * * * * * * * *

I would be very interested in any of your thoughts on this subject. I'd be happy to summarize the responses to the net.

Barry A. Stevens, Applied AI Systems, Inc., PO Box 2747, Del Mar, CA 92014
619-755-7231

Risks of Portable Computers

Peter G. Neumann <NEUMANN@csl.sri.com>
Thu 3 Dec 87 09:13:14-PST

Northwest Airlink had a real computer crash. A 50-pound personal computer belonging to a passenger, Ron Olstad, fell from a cargo pod on a Jet Stream 31 commuter plane landing in Oshkosh, Wisconsin. The computer crash landed into Ronald Miller's backyard. Northwest Airlink replaced the computer. [but not the divot!]

From the International Herald Tribune, 18 November 1987, p.3, courtesy of Vicki Almstrum of Philips in Jarfalla (with `"' over the first two `a's).

Beware the Temporary Employee

Howard Israel <HIsrael@DOCKMASTER.ARPA>
Thu, 3 Dec 87 11:09 EST

BLUE CROSS ISSUES RED-FACED APOLOGY (Bergen Record, 12/2/87)

UPI, Providence, R.I.- A mysterious prankster has struck Blue Cross and Blue Shield of Rhode Island and about 100 of its subscribers. The subscribers recently received letters from the health insurer concerning doctor bills, with a postscript that would confirm the worst fears of many subscribers. It read, "Note: Your eligible charges will remain in file until hell freezes over."

Red-faced Blue Cross officials apologized to subscribers for the blooper but have not been able to find the culprit. A temporary employee who had access to the computer that generated the letter left the day the sentence was added, a spokesman said Monday.

truncated anything

Doug Mosher <SPGDCM%cmsa.Berkeley.EDU@ucbvax.Berkeley.EDU>
Thu, 03 Dec 87 18:02:20 PST

Following the discussions of truncating UNIX keywords to 8 characters without notice, I would like to make the following statement/opinion/recommendation:

It is ALWAYS BAD PRACTICE to delete anything without notice.

One special case of this is:

It is ALWAYS BAD PRACTICE to truncate anything without notice.

Many examples over the years occur to me; here's a small partial list.

Several products provide a really gimpy form of "Artificial Intelligence" by allowing the user to insert meaningless words, and ignoring them without notice.

Example: syntax would be: "print amount by state by city".
Syntax also allowed: "please print me a report showing the amount sorted by state and then by city".

This starts off looking good, but ends up deleting all sorts of necessary keywords if you ever slip and misspell them, with very hazardous outcomes. You get a report, all right; no messages are issued; you go ahead and buy things/fire people/explode bombs, based on the WRONG REPORT RESULTS.

Products which do this include FOCUS and TELL-A-GRAF.

Some Microsoft BASIC interpreters give the impression of allowing variable names longer than 2 characters, but actually they just truncate to two characters. This results in VERY PAINFUL and hard to find bugs, when one finally calls two things PRINT and PRACTICE or whatever.

The IBM Pl/I compiler truncates variable names to 31 characters. This is longer than most people are motivated to use so it has rarely caused anyone pain. External names are truncated to 8 characters, but at least notice is given.

IBM MVS dataset names are truncated at 44 characters. This is not a frequent source of problems, but many folks have tripped over this at one time or another. To compound things, under various circumstances in the MVS operating system, dataset names are further shrunk to lengths such as 22, inside tape label fields, or in certain types of catalogs. The rule chosen is to cut stuff out of the middle, which is better than cutting it purely off either end, but eventually somebody makes themselves exactly the right size and shape and falls off this cliff.

Early IBM VM/CMS command and exec languages tokenize everything to 8

characters, discarding excesses. On the one hand, this is somewhat less hazardous, since it is so pervasive and widespread; but it still causes problems. (For one thing, frequent users tend to reduce their entire vocabulary to words of 8 letters or less, both a good and a bad effect.... I really was doing this for awhile!). The currently preferred script language, REXX, avoids this problem, but EXEC I and EXEC II are still in use and still do it.

The problem was especially pernicious in certain circumstances. For example, if you wanted to save a token and compare it, you had to concatenate a period on the front, because it might be missing, and without at least the period, you'd get syntax errors in a comparison. But then, you were limited to 7 "real" characters, the eighth one having been pushed off the right hand end and truncated without notice...

Doug Mosher, 257 Evans, Univ. of California, Berkeley, CA, 415/642-5823

An ancient computer virus

Joe Dellinger <joe@hanauma.STANFORD.EDU>
Wed, 2 Dec 87 00:14:25 pst

In 1982, while a student at Texas A+M University, I created a Virus for Apple][Dos 3.3. I was curious to see how long it would take for such a virus to spread through my own disk collection, so I was very careful to make the virus completely harmless (and indeed even completely undetectable). I was very careful to operate under strict quarantine. Unfortunately, several friends let the virus escape, before I was through perfecting it. The earlier versions of virus would cause the graphics in a certain game to smear. Within a few weeks, everybody's (pirated) copy of this game (called "Congo") stopped working. To correct this situation, we launched another "perfected" virus to displace the first. As it turned out, the "perfected" virus worked well, and so I never heard from it again.

Are Apple][' s running 64K Dos 3.3 still being used? If so, it might make an interesting study to see how much this virus has spread in 5 years. If the virus is in memory, there will be a short ASCII text string listing the generation count starting at location $B6E8 in memory. Normal DOS has zeroes there.

Cable violations of privacy (Re: RISKS-5.66)

<rogers%ncrcce%ncrlnk.dayton.ncr.com@RELAY.CS.NET>
Thu, 3 Dec 87 01:34:54 -0500 (at ncrlnk.Dayton.NCR.COM)

People concerned about violations of privacy may be interested in the following comments from Peter Barton, executive vice president of the Cable Value Network (CVN - a shop-via-TV retailer) as quoted in the Minneapolis Star Tribune Sunday magazine:

"We got your name. We know where you live. We know something about what your life style may be all about. We know what you bought, so we're going to

start sending you catalogs. ...This business is a manifestation of the evolution of data transmissions by satellites and the capacity to manage as much data as you can. You couldn't have done this business five years ago. These computers weren't powerful enough. It really is the right business at the right time. It's kind of fun."

Bob Rogers, NCR Comten, St. Paul, MN

Re: Computer-controlled train runs red light (RISKS-5.65)

<ucbcad!ames.UUCP!hoptoad!academ!nuchat!steve@ucbvax.Berkeley.EDU>
2 Dec 87 22:19:44 CST (Wed)

(Steve Nuchia)

> Technical experts agree that microprocessor-based systems are more flexible
> in operation and much better at monitoring and fault diagnosis than the
> relay-based systems they typically replace. ...

> Symposium participants expressed concern, however, about the probablity
> of failure of the microprocessor in an unsafe way as a result of inadequate
> verification of its software.

Perhaps there is a risk inherent in technological progress - the consumers of the technology come to expect continued rapid progress, without regard for engineering reality.

The pair of statements quoted above are an example of such inflated expectations, and the disappointment that usually accompanies inflated expectations. Here we have a bunch of engineers lamenting the lack of reliability in electronic digital control system, as compared against relay based controls. But no mention is made of hardware reliability!

Surely these engineers can't be so paranoid as to think that an exact duplication of their (primarily digital) relay-based control system in software would be hard to verify. It should at least be possible to build a software implementation that could be easily shown to be equivalent to the relays, leaving aside the problem of validating an arbitrary "spagetti code" implementation.

Which brings us to the first excerpt, in which the "chips" are lauded for being more flexible and having more functionality than the relays. So, we are comparing an expensive and mechanically failure-prone solution against a less expensive solution prone to mysterious bugs and a different breed of hardware faults. Trouble is, the two solve different problems!

Why is the computerized solution expected to do everything the relay box did, plus diagnose itself and be "more flexible in operation" (whatever that means exactly), at a lower cost and with no technology-specific risks? At least these people were responsible and alert enough the realize that they had expectations that the technology couldn't meet before putting it into production.

Automobile traffic light control boxes, based on relay technology quite similar to that used in railroads, fail every so often due to ants building mounds in the nice warm cabinets. People have been killed by this bug in a relay system, yet it fails to generate the kind of emotional response that software bugs do. ---

Steve Nuchia (713) 334 6720

VM systems vulnerability

<Doug Mosher>
Fri, 04 Dec 87 14:15:46 PST

The following has come out in VMSHARE, a national bulletin board for IBM VM systems programmers. It is in a file "PROB SECURITY", which is only available to those on a specific prearranged access list.

(Note: the number 2600 derives, I believe, from a frequency that was widely used in earlier days by blue boxes to permit unpaid long-distance calls.)

==========

Append on 12/03/87 at 23:49 by Thomas P. Owens - (907)-276-7600:

VM has, at long last, arrived! 2600, the Monthly Journal of the American Hacker, devoted the better part of seven pages (November 1987) to an article "Hacking IBM's VM/CMS". The information given is dead(ly) accurate, so far as it goes.

I urge one and all to review your anti-hacking measures. If you don't have any such measures, this would be a GOOD time to mend your ways. If your management is a bit slow to respond to exposures, drop them a broad hint that there is at this very moment a crew of anti-social computer weenies loose in your neighborhood. At worst, the statement is literally true; at best, a benevolent "foma".

Doug Mosher, 257 Evans, Univ. of California, Berkeley, CA, 415/642-5823

Baby monitors end up 'bugging' the whole house

Shane Looker <shane@pepe.cc.umich.edu>
Wed, 2 Dec 87 12:46:26 EST

By : Constance Prater
Original : The Detroit News -- Nov 22, 1987, Section B, page 1
Copied without permission.

When 9-month-old Detroiter Bradley Dunn cries, a lot of people may hear him. And that "bugs" his mother, Ellen. But the fact is, Bradley's nursery is bugged. Dunn recently put an inexpensive baby monitoring transmitter in Bradley's room so she could hear him on a receiver she carries throughout the house. What she didn't realize was that now any neighbor with a low-frequency electronic receiver, or walkie-talkie, can eavesdrop on

Bradley -- or any other household activity.

Electronic eavesdropping is a federal [USA] no-no, and upon conviction under the Electronic Communications Privacy Act of 1986, violators can be sentenced to a year in prison and fined $100,000. The law makes it illegal to intercept, listen to, or disclose information from private electronic signals. But federal agents won't be out tracking down neighborhood listeners, said John Anthony, special agent in Detroit's FBI office. "From a practical standpoint, how do you enforce something like that?" he said. "We're not going down to investigate baby monitor listeners."

A half-dozen toy companies manufacture the baby monitoring and intercom devices, including a nationally advertised medel made by Fisher-Price Toys. The units operate in a frequency range of 30 to 50 megahertz. Under the right conditions, they can carry baby gurgles or any other sounds in a room on low-frequency airwaves to receivers as far away as a quarter of a mile.

Congress probably didn't have baby monitors in mind last year when it wrote the federal law intended to prevent wiretapping, electronic listening devices and cabbies stealing each other's fares. But the nursery listening aids are, in a sense, "bugs", too. "You never think that your neighbors could be listening to you through a baby monitor," said Fran Ganim of Livonia, who bought a Gerry Deluxe model monitor in August just before the birth of her daughter. "I guess we have to watch what we say."

A Taylor man, who owns a Radio Shack PRO 2020 scanner receiver to monitor police and emergency rescue channels, said he suspected he was breaking the law when he listened to a husband and wive arguing and yelling at their children. "I can pick up everything that's going on in their house," said the man, who spoke on condition that his name not be used. He said that after he also heard a small child crying, he figured out the signal he'd accidentally locked in on was from a baby monitor. He traced the signal to a home a half-block away and eventually told his neighbors about their lack of privacy.

Baby monitors, beepers, pagers, office intercoms, cordless and car telephones and walkie-talkies all emit electronic signals. The devices can transmit or receive signals from each other in close range, or be picked up on more powerful receivers capable of scanning lower frequencies.

Electronics technology has improved faster than legislatures can make laws regulating the equipment's use, the FBI's Anthony said. "Anybody with a little bit of knowledge and a lot of time on their hands ... can go to Radio Shack or another electronics store, get some pretty ophisticated equipment and listen to just about anything they want," he said. "When you throw it (a transmitting signal) up there in the ionosphere, anybody can hear you."

The Federal Communications Commission (FCC) requires label warnings only for users of cordless telephones, which use shared frequencies, said Richard Engleman, and FCC electronics engineer. "Communications are intended to be private. I would be upset if somebody was listening to me," Engleman said. He said electronic interception is a difficult area to regulate, citing satellite dishes as an example. "A lot of people maintain the airwaves are free to use. And what comes into my home is fair game," he said.

F4 in 'Nam (Re: Reversed signal polarity causing accidents)

Brent Chapman <chapman%mica.Berkeley.EDU@violet.berkeley.edu>
Mon, 30 Nov 87 23:06:07 PST

In Risks-5.66, Clive D.W. Feather <mcvax!root.co.uk!cdwf@uunet.uu.net> writes of how reversed polarity in a rail switching relay led to an accident that killed two people.

This reminds me of story I heard about the American F4 fighter in its early days of service in VietNam. I heard the story from an Air Force colonel who flew that aircraft in VietNam; I don't know if he was being completely honest with me or not, but it seems plausible.

During an ejection, the charges that separate the canopy are supposed to explode a split second before the charges that propell the ejection seat out of the aircraft. In these early F4's, there was apparently about a 50-50 chance that the sequence would happen the other way around (the seat would fire before the canopy did), causing the pilot to be ejected through the still-intact glass canopy, usually seriously or fatally injuring the pilot. The culprit was a wiring harness plug in the ejection control system that could be connected (with proper and common application of main force) so that the "blow-canopy" and "blow-seat" lines were reversed, causing the order of firing to be reversed. When the problem was finally diagnosed, the plugs were all replaced with ones that supposedly _couldn't_ be reversed.

An interesting side note: the low-tech means that the pilots developed to deal with the problem between the time they decided it _was_ a problem and the somewhat later time that it was "fixed" was to wire a pair of bayonets to the "rails" on either side of the ejection seat so that the points projected above the pilot's head. That way, if the seat blew before the canopy, the canopy would be shattered by the knives instead of by the pilot's head.

Brent Chapman chapman@mica.berkeley.edu or ucbvax!mica!chapman

IRS computers (yet again!)

Joe Morris (jcmorris@mitre.arpa) <jcmorris@mitre.arpa>
Wed, 02 Dec 87 08:50:20 EST

The following short item appeared on p. 1 of the 25 November issue of _The_Wall_Street_Journal_; it's copied in its entirity, and as usual without permission:

> DON'T BLAME US. It's our naughty computer that keeps breaking the law.
>
> The law tells the IRS to wait 90 days after issuing a deficiency

notice before trying to collect. If a taxpayer takes the matter to Tax Court, the IRS must hold off until the case is resolved. Yet, soon after Paul and Gina Husby proceeded to Tax Court, the IRS billed the San Francisco couple $47,000. A computer error, an IRS attorney assured them; don't worry.

But more bills came, and the agency grabbed nearly $3,800 in Paul's credit union. Even after a federal court ordered a halt, the unlawful collection action went on. Finally, the IRS curbed itself, returned the credit union money, but argued the Husby's lawsuit for damages should be summarily dismissed. District Court Judge Weigel recently noted that the IRS "position boils down to the contention that the whole unfortunate incident was really nobody's fault, but the computers'."

That won't let the agency off the hook, the judge said, ruling that the case should proceed to trial.

Call for papers -- JOURNAL OF COMPUTING AND SOCIETY

Gary Chapman <chapman@russell.stanford.edu>
Thu, 3 Dec 87 14:35:53 PST

CALL FOR PAPERS
FOR DEBUT ISSUE
of
THE JOURNAL OF COMPUTING AND SOCIETY

Ablex Publishing Corporation will begin quarterly publication of a new academic journal on the social implications of computing technology in late 1988 or early 1989. The purpose of The Journal of Computing and Society will be to stimulate lively debate and speculation on a wide variety of topics concerning the computerization of society. The journal will be refereed. When it begins publication, individual subscriptions will be encouraged, and it should be available on stands in quality bookstores.

Issues of the journal will be organized around themes. The first theme is "Has There Been A Computer Revolution?" Contributors are encouraged to submit papers relating to this theme (not necessarily answering the question yea or nay). Papers for this issue should be received by April 15, 1988. Future themes will include computers and war, computers and privacy, risks to the public, computers and power, the computer as metaphor, computers and gender, etc. Suggestions for themes are welcome, and the journal will publish a few articles outside the theme if the papers are of signficant quality, timeliness, and relevance to the purposes of the journal.

Manuscripts should be 10-20 pages in length, conforming to the Chicago Manual of Style, and submitted in quadruplicate. A sheet of information for authors is available from the editor.

The editor of this journal is Gary Chapman, executive director of Computer Professionals for Social Responsibility. Manuscript submissions and all

correspondence should be directed to him at P.O. Box 717, Palo Alto, CA 94301. The telephone number is (415) 322-3778.

The current editorial board of The Journal of Computing and Society consists of the following people:

Search RISKS using swish-e

THE RISKS DIGEST

Forum on Risks to the Public in Computers and Related Systems

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

Volume 5: Issue 70

Sunday, 6 December 1987

Contents

Wall Street crash, computers, and SDI

Rodney Hoffman <Hoffman.es@Xerox.COM>
6 Dec 87 12:29:47 PST (Sunday)

From the 'Letters' column in the 'Wall Street Journal', Thursday, Dec. 3, 1987:

SDI COULD BE TOO SWIFT

The role of computers in the recent wide fluctuation of stock prices brings to focus an interesting issue that has wider implications. The initial downward trend in the market was greatly amplified by rapid computer-initiated program trading. From our long experience in computer science and dynamical systems analysis, we fear that this dangerous amplification effect could occur in other more critical computational networks, most notably those envisioned for the strategic defense initiative (SDI).

SDI planners have proposed giving computers a key role in the decision about retaliatory measures in the event of attack. Others have argued persuasively that a computer program that reflects our policy cannot be reliably constructed or completely debugged. But setting this aside, we claim that there would be great danger in the very speed of such programs, unmodulated by slower hauman interactions that provide effective damping. It is known that nonlinear systems (such as the ones composing computer networks) can amplify very small disturbances. As illustrated by the program trading example cited, this can cause massive changes in overall system behavior unplanned for by system designers.

The programs in the defense network for SDI must process incoming signals for possible threats, and act rapidly in accord with the resulting analysis. Any overt action by the SDI system can lead to a rise in the readiness of the opposite side; blasts in space can be interpreted by Russian programs as attacks on spy satellites, a preparatory move for a U.S. first strike. This automatic feedback loop, through the Russian and American computers and sensors, can easily amplify the intesity of a dangerous situation to the point of nuclear catastrophe. In order to dampen such an inadvertent escalation, humans must be involved in the response progress, even at intermediate stages. They must have time enough to think and communicate to avoid the nonlinear amplification effects. In the case of the envisioned system for SDI, we believe that there is no effective way whereby people can modulate the behavior of a computer system while retaining the hoped for rapid response.

Daniel G. Bobrow
Bernardo A. Huberman
Palo Alto, Calif.

(NW Flight 255) Simulator did, but wasn't.

Scot E. Wilcoxon <umn-cs!datapg.MN.ORG!sewilco@cs-gw.D.UMN.EDU>
Thu, 3 Dec 87 13:36:36 CST

The random failure of a $13 circuit breaker may have contributed to an airplane crash. Also, an indicator in the simulator for the aircraft behaves differently than in the real aircraft when that failure occurs.

Northwest Flight 255 apparently crashed in Detroit three months ago because the flaps were not lowered during takeoff. The MD 80's takeoff warning system should have warned the pilot, but its audio warning "flaps, flaps" was not on the cockpit recording so the warning system probably failed.

NTSB examination of a $13 circuit breaker that supplies power to the

warning system has found several planes with breakers that would not pass the electrical current that they should.

A McDonnell Douglas document states that when power fails to the warning system, a warning light (CAWS fail light) should go on in the cockpit. That is what happens in the MD80 simulator, but in an actual MD80 aircraft the warning light does not go on.

A McDonnell Douglas official said the document is "clearly in error". (quoting StarTribune:) "This revelation has put the FAA in the awkward position of ordering changes that will make the simulators behave the same way as the airplane instead of making the airplane behave like the simulator."

The simulator will be altered instead of airplanes because the warning system is classified by the FAA as not requiring backup systems. The warning system is required (FAA won't allow takeoff if it is not working), but is considered "nonessential" for manufacturing purposes (FAA does not require backup systems for nonessential systems).

(Information from 11/28/87 Minneapolis Star Tribune, pg 1,4D)

Scot E. Wilcoxon sewilco@DataPg.MN.ORG {ems,meccts}!datapg!sewilco
Data Progress Minneapolis, MN, USA +1 612-825-2607

Whistle-blowers who aren't

<mnetor!utzoo!henry@uunet.UU.NET>
Wed, 2 Dec 87 15:47:52 EST

> Maxson will share the stage with former Morton Thiokol engineer Roger
> Boisjoly, who currently has a billion-dollar suit underway...

Maybe I am just being picky about this, but it still makes me see red when I see Boisjoly described as a "whistle-blower". Boisjoly is the man who could have blown the whistle BUT DIDN'T, and seven astronauts died as a result. Boisjoly was the engineer who told MT management "don't launch", was told "put on your management hat", did so, and changed his expert professional opinion 180 degrees to match his hat color. In a just world, I cannot help but think that he (and, certainly, his management) would be facing criminal charges. Boisjoly did not blow the whistle; he merely turned "state's evidence" after the fact.

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

---

Re: Space Shuttle Whistle-Blowers Sound Alarm Again (reprint)

<mnetor!utzoo!henry@uunet.UU.NET>
Wed, 2 Dec 87 15:48:00 EST

> ... new and improved shuttle escape mechanisms. Lot's of
> money is being spent, but whether reported or not, upon (close) examination

> none of these mechanisms would prevent the death of astronauts in a
> Challenger type disaster. I wonder just how much additional engineering
> is happening for purely public relations purposes...

The escape work is not being done for purely public relations purposes; it merely, for the most part, does not address situations as severe as the Challenger disaster. There is in fact some attention being given to such situations, but the thorough re-examination of shuttle safety issues turned up other cases where modest effort would yield a much higher probability of survival. The reason why most escape-system work is not addressing the Challenger scenario is that it is very difficult to get the crew out of such a situation reliably! There are also tradeoffs to be considered: regardless of managerial idiots blithering about safety being an absolute priority, the only way to make the shuttles completely safe is to put them in museums and never fly them again. In practice, there is no way to avoid some level of compromise between safety and utility, since adding any type of escape system reduces payload. There are also safety-vs-safety tradeoffs to be made, since even simple ejection seats can and do fire accidentally, often with fatal consequences.

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

---

A new twist to password insecurity (human factors)

Roy Smith <roy%phri@uunet.UU.NET>
6 Dec 87 00:19:06 GMT

A bunch of people around here have signed up for the BRS/Colleague bibliographic data base service. Each person has an individual account number and (supposedly secret) password. We get a combined invoice each month, with usage itemized and identified, but only by account number (not by name). Our accounting office didn't know what to do with the account numbers, so I called BRS and asked for a list of which name corresponds to which account number. Much to my surprise, I got in the mail a few days later a list of names, account numbers, *and passwords*.

Roy Smith, {allegra,cmcl2,philabs}!phri!roy
System Administrator, Public Health Research Institute
455 First Avenue, New York, NY 10016

More on PIN encoding

Chris Maltby <munnari!softway.oz.au!chris@uunet.UU.NET>
2 Dec 87 11:47:01 +1100 (Wed)

A recent fraud case in Sydney reveals that the PIN details are either encoded on the card, or a function of the card number. The perpetrators of the fraud used some ingenuity in their system.

The first stage was to deduce the magnetic encoding on the card's strip from discarded receipts collected around ATMs, and then manufacture cards which

duplicated the real card. Unfortunately for them, they were unable to break the PIN encoding algorithm, so they resorted to hanging around in their cars opposite the ATM location with a portable video camera and a zoom lens. When some unsuspecting user left behind a recipt card they were able to re-manufacture his card and replay the video of his PIN entry.

There are several morals. First - don't leave your receipts at the machine. Second - stand close when entering your PIN. Third - don't use the system at all - can you trust any system which is this easy to break. If the forgers had been just a bit more resourceful they would have decoded the PIN as well. Of course, the "conditions of use" of your card make you liable for such frauds...

Chris Maltby - Softway Pty Ltd (chris@softway.oz)

PHONE: +61-2-698-2322 uunet!softway.oz!chris chris@softway.oz.au

---

Telephone overload (Re: RISKS-5.63)

Stephen Grove <ptsfa!pbhya!seg@ames.arpa>
Wed, 2 Dec 87 16:09:35 PST

> Date: Fri, 20 Nov 87 15:17:09 PST
> From: "LT Scott A. Norton, USN" <4526P%NAVPGS.BITNET@wiscvm.wisc.edu>
> Subject: L.A. Earthquake & Telephone Service
>
> Can anyone with better knowledge of the phone companies' local offices tell
> me if there is some simple way to shed this extra load in a reasonable way?
> I know that after some minutes off the hook, the phone loses its dial tone.
> Does this adequately release the resources the off-the-hook phone was using?

The older electromechanical systems, required someone to throw a switch and remove the battery supply from the non-priority customers.
Priority-customers being those in the class of Hospitals, Police, Fire, etc.

The newer ESS offices (ESS = Electronic Switching Systems, using stored programs for control, as opposed to hard-wired logic) determine when the load is getting excessive, and delay the response to nonpriority customers by a factor of three (I think). In other words if the ESS normally responds in 300ms, it will now take 900ms. I have seen it work in a flood, and it worked fine. It was inhibited at first, and the ESS repeatedly stated the need to implement the control, and was unable to serve anyone, but when allowed, response was slower, but the calls went through.

For call in programs and promotions, we like to provide special prefixes that can be limited in the number of interoffice channels they can access.

Stephen Grove, Pac Bell, Rohnert Park, Calif.
UUCP:{ihnp4,dual,sun,hoptoad}!ptsfa!pbhya!seg

Software licensing problems

Geof Cooper <imagen!geof@decwrl.dec.com>
Wed, 2 Dec 87 12:47:00 pst

We too have experienced the problem of software licensed to run on only some nodes. Our approach has been to convince the repairman types to switch the Node-ID rom's on the apollos in question, so that your access key follows you where you go. I've never seen the address ROM itself fail!

Apollo Computer has recently brought out a product that allows N copies of a program to be running simultaneously on any of some larger number of machines. It remains to be seen if any vendors will be interested in using the product. From the vendors' point of view, there is a possible financial risk to adopting the new scheme, since many programs are used less than full time; the customer might elect to buy fewer copies of the program and take the risk that occasionally someone will have to "wait for a dialtone". E.g., we have about 25-30 licenses for Interleaf's desktop publishing software. I've never seen more than 15 of them in use at once).

- Geof

Re: Mariner 1 or Apollo 11? (RISKS-5.63)

<mnetor!utzoo!henry@uunet.UU.NET>
Wed, 2 Dec 87 15:48:18 EST

> I heard that the famous "./," disaster caused the problem with the
> onboard IBM 1800 on Apollo 11...

The onboard computers on Apollo were not IBM 1800s unless I have confused the numbers badly, and almost certainly they were programmed in assembler due to severely limited ROM capacity, so I'd be a bit skeptical of this.

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

Re: Mariner 1 or Apollo 11?

Brent Chapman <chapman%mica.Berkeley.EDU@violet.berkeley.edu>
Mon, 30 Nov 87 22:26:10 PST

In RISKS-5.64, Scott Dorsey <kludge@pyr.gatech.edu> writes:

> I heard that the famous "./," disaster caused the problem with the
>onboard IBM 1800 on Apollo 11. I heard this from a professor who teaches
>Fortran, so I'm not so sure about the reliability of the source. Anyone
>else have information on either the Apollo or the Mariner problems?

If you mean the "decent alarm" that occurred in the Lunar Module moments before lunar touchdown, then one of the NASA documentaries (unfortunately, I don't remember the title, or even when or where I saw it) told a different

story. They said that the alarm was caused by an overload condition in the processor; apparently the Armstrong and Aldrin had left a certain sensor (radar altimiter, I think) enabled that was supposed to have been shut down by that point in the landing sequence, and the added load of that sensor caused the computer to falsely register an alarm condition. If I remember correctly, the programmer that had written the piece of code involved was in Mission Control at the time the alarm occurred; he stared at the situation and status boards for a few seconds, then announced that he knew what the problem was, that it was a false reading, and advised to continue the landing (although I'm not sure if they could have aborted at that stage or not).

I may be confusing what I saw in the documentary (that the false decent alarm happened because the processor was overloaded because a sensor that should have been turned off wasn't) with "urban legend" (that the programmer responsible was in Mission Control, etc.); can anyone else back me up on this?

Brent Chapman Capital Market Technology, Inc.
Senior Programmer/Analyst 1995 University Ave., Suite 390
{lll-tis,ucbvax!cogsci}!capmkt!brent Berkeley, CA 94704
capmkt!brent@{lll-tis.arpa,cogsci.berkeley.edu} Phone: 415/540-6400

[I am sorry that misinformation is still flowing on this subject. I have held up a large number of potential contributions to RISKS, awaiting a definitive report that is rumored to be working its way RISKSward. PGN]

More on addressable converter box

Allan Pratt <ucbcad!ames.UUCP!atari!apratt@ucbvax.Berkeley.EDU>
Mon, 30 Nov 87 11:40:31 pst

RISKS@KL.SRI.COM (RISKS FORUM, Peter G. Neumann -- Coordinator):

I have a note to add about my addressable converter box: the hardware is two-way capable. I know this because there is an "event" button which you hit to purchase an event on Pay-Per-View. You then key in your purchase-authorization code, and you get the event. Obviously, the box has to be two-way, because the cable company has to be able to bill you. Now, the particular cable company in my area does not support this, but the box hardware & software do. The manual talks about it, with an "If your cable company supports it" disclaimer.

Opinions expressed above do not necessarily -- Allan Pratt, Atari Corp.
reflect those of Atari Corp. or anyone else. ...ames!atari!apratt

---

centralized car locks (foaf)

K. Richard Magill <umix!oxtrap!rich@RUTGERS.EDU>
30 Nov 87 18:17:47 GMT

It's my understanding that a certain lesser known car (the Bricklin) was sold with entirely electronic locks. When the battery died or shorted you

were entirely locked out. The Bricklin had gull wing doors.
rich.

[When the gulls attacked, the car owners
were known as the Bricklin drudgers. PGN]

Search RISKS using swish-e

THE RISKS DIGEST

Forum on Risks to the Public in Computers and Related Systems

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

Volume 5: Issue 71

Monday, 7 December 1987

Contents

The Amiga VIRUS (by Bill Koester)

Bernie Cosell <cosell@WILMA.BBN.COM>
Mon, 7 Dec 87 0:25:23 EST

From: bill@cbmvax.UUCP (Bill Koester CATS)
Newsgroups: comp.sys.amiga
Subject: Amiga VIRUS

Date: 13 Nov 87 19:32:05 GMT
Organization: Commodore Technology, West Chester, PA

THE AMIGA VIRUS - Bill Koester (CATS)

When I first got a copy of the Amiga VIRUS I was interested to see how such a program worked. I dissassembled the code to a disk file and hand commented it. This article will try to pass on some of the things I have learned through my efforts.

1) Definition. 2) Dangers. 3) Mechanics 4) Prevention

1. - Definition.

The Amiga VIRUS is simply a modification of the boot block of an existing DOS boot disk. Any disk that can be used to boot the Amiga (ie workbench) has a reserved area called the boot block. On an Amiga floppy the bootblock consists of the first two sectors on the disk. Each sector is 512 bytes long so the boot block contains 1024 bytes. When KickStart is bringing up the system the disk in drive 0 is checked to see if it is a valid DOS boot disk. If it is, the first two sectors on the disk are loaded into memory and executed. The boot block normally contains a small bit of code that loads and initializes the DOS. If not for this BOOT CODE you would never see the initial CLI. The normal BOOT CODE is very small and does nothing but call the DOS initialization. Therefore, on a normal DOS boot disk there is plenty of room left unused in the BOOT BLOCK.

The VIRUS is a replacement for the normal DOS BOOT CODE. In addition to performing the normal DOS startup the VIRUS contains code for displaying the VIRUS message and infecting other disks. Once the machine is booted from an infected disk the VIRUS remains in memory even after a warm start. Once the VIRUS is memory resident the warm start routine is affected, instead of going through the normal startup the VIRUS checks the boot disk in drive 0 for itself. If the VIRUS in memory sees that the boot block is not infected it copies itself into the boot block overwriting any code that was there before. It is in this manner that the VIRUS propagates from one disk to another. After a certain number of disks have been infected the VIRUS will print a message telling you that Something wonderful has happened.

2. - Dangers.

When the VIRUS infects a disk the existing boot block is overwritten. Since some commercial software packages and especially games store special information in the boot block the VIRUS could damage these disks. When the boot block is written with the VIRUS, any special information is lost forever. If it was your only copy of the game then you are out of luck and probably quite angry!!

3. - Mechanics.

Here is a more detailed description of what the virus does. This is intended to be used for learning and understanding ONLY!! It is not the authors intention that this description be used to create any new strains of the VIRUS. What may have once been an innocent hack has turned into

a destructive pain in the #$@ for many people. Lets not make it any worse!!

a.) Infiltration.

This is the first stage of viral infection. The machine is brought up normally by reading the boot block into memory. When control is transferred to the boot block code, the virus code immediately copies the entire boot block to $7EC00, it then JSR's to the copied code to wedge into the CoolCapture vector. Once wedged in, control returns to the loaded boot block which performs the normal dos initialization. Control is then returned to the system.

b.) Hiding Out.

At this point the system CoolCapture vector has been replaced and points to code within the virus. When control is routed through the CoolCapture vector the virus first checks for the left mouse button, if it is down the virus clears the CoolCapture wedge and returns to the system. If the left mouse button is not pressed the virus replaces the DoIO code with its own version of DoIO and returns to the system.

c.) Spreading.

The code so far has been concerned only with making sure that at any given time the DoIO vector points to virus code. This is where the real action takes place. On every call to DoIO the virus checks the io_Length field of the IOB if this length is equal to 1024 bytes then it could possibly be a request to read the boot block. If the io_Data field and A4 point to the same address then we know we are in the strap code and this is a boot block read request. If this is not a boot block read the normal DoIO vector is executed as if the virus was not installed. If we are reading the boot block we JSR to the old DoIO code to read the boot block and then control returns to us. After reading, the checksum for the virus boot block is compared to the checksum for the block just read in. If they are equal this disk is already infected so just return. If they are not equal a counter is incremented and the copy of the virus at $7EC00 is written to the boot block on the disk. If the counter ANDed with $F is equal to 0 then a rastport and bitmap are constructed and the message is displayed.

d.) Ha Ha.

< Something wonderful has happened >
< Your AMIGA is alive!!! >
< and even better >
< Some of your disks are infected by a VIRUS >
< Another masterpiece of the Mega-Mighty SCA >

4. - Prevention.

How do you protect yourself from the virus?

1) Never warm start the machine, always power down first.
(works but not to practical!)

2) Always hold down the left mouse button when rebooting.
(Also works, but only because the VIRUS code checks for
this special case. Future VIRUS's may not!)

3) Obtain a copy of VCheck1.1 and check all disks before use.
If any new virus's appear this program will be updated and released
into the public domain. VCheck1.1 was posted to usnet and will
also be posted to BIX.
(Just like the real thing the best course of action is
education and prevention!)

Bill Koester -- CBM <>Amiga Technical Support<<
UUCP ...{allegra|burdvax|rutgers|ihnp4}!cbmvax!bill
PHONE (215) 431-9355

Radar's Growing Vulnerability

Peter G. Neumann <NEUMANN@csl.sri.com>
Mon 7 Dec 87 13:52:21-PST

For readers of SCIENCE, the 27 November 1987 issue (p. 1219) has a nice article by Stephen Budiansky (titled asa the Subject line above) on the problems of defensive radars. ``As weapons become smarter, they learn to "see" radar beams as pathways to their target, gaining an advantage over defensive systems.'' The caption on a picture of the smoking HMS Sheffield says that it ``was hit in the Falkland Islands war in 1982 when its radars attracted a rocket launched from a fighter plane 20 miles way.'' (RISKS readers will recall that the British investigation concluded that the Sheffield's own radars were jammed by a communcation back to London that was being held at the time.)

Computerized vote counting

Lance J. Hoffman <LANCE%GWUVM.BITNET@WISCVM.WISC.EDU>
Mon, 7 Dec 1987 14:22 EST

I have just completed a study of computerized vote-counting systems. The report, based on a workshop of experts in election administration and computer security, presents recommendations to improve the security and reliability of computerized vote-counting systems. The recommendations are organizational, not technical, because that is where the most important problems lie. However, five focus papers are included, including one by Willis Ware on "A Computer Technologist's View". For a free copy, please send a snail mail or email request with your complete snail mail address to

Election Computer Security Project

Dept of Electrical Engineering & Computer Science
The George Washington University
Washington DC 20052

Lance Hoffman (LANCE@GWUVM.BITNET)

United Airlines O'Hare Sabotage?

Chuck Weinstock <weinstoc@SEI.CMU.EDU>
Mon, 07 Dec 87 17:36:28 EST

On December 3, I was traveling from California to Pittsburgh via Chicago on United. My inbound flight came in at an E gate and my outbound left from a new C gate. If an agent hadn't been there to greet the plane, I wouldn't have known it because the monitors were out. I got to the C terminal and the monitors there were on but unreadable due to jiggle (all of them.) I went to a pay phone and could not get a dial tone (on any of them.) I boarded my flight and we sat for an extra 20 minutes because "a cable had been cut" and thus they were unable to calculate the amount of fuel to load. I surmised that this was a landside cable and that all of the above events were somehow related.

I decided to call United today and learned that my surmise was true. Multiple fires in the basement of terminal 2 caused both AT&T and United wires to be severed. The former knocked out the pay phones, and the latter the airline's ability to communicate with it's computers across town.

It also seems that, at the new terminal at least, there is an automatic, underground fueling system which shut off once it detected a fire. Technicians were able to override the interlock once they determined that there was no danger due to the fire, and the pilots apparently had to do fuel calculations manually. Given that United has a new computerized baggage routing system at O'Hare, I'm really surprised that my luggage made the connection ok.

175 flights were delayed on Thursday and Friday morning. Officials suspect arson though the United spokesman I talked to could not suggest a motive. Full phone service to the terminal was not restored until Friday evening. United is awaiting licensing of a microwave system in the near future to leave themselves less vulnerable to this sort of sabotage.

Re: Whistle-blowers who (allegedly) aren't

Jeffrey Mogul <mogul@decwrl.dec.com>
7 Dec 1987 1646-PST (Monday)

Henry Spencer writes:

> Maybe I am just being picky about this, but it still makes me see red when I see Boisjoly described as a "whistle-blower". Boisjoly is the man who could have blown the whistle BUT DIDN'T, and seven astronauts died as a result. Boisjoly was the engineer who told MT management "don't launch", was told "put on your management hat", did so, and changed his expert

professional opinion 180 degrees to match his hat color...

I recently saw a videotape of Boisjoly's appearance at MIT. I think Henry is somewhat confused; Boisjoly made it quite clear that it was another person (higher up in the management structure) who was told to "put on your management hat" and who in fact reversed his engineering opinion (and, as I recall, that was enough to overrule the other engineers). True, Boisjoly did not blow the whistle (i.e., go outside Morton Thiokol) at this point, but he says that he and other engineers were quite upset at the time, and he referred to a notebook entry he made that night expressing his fear about the next day's launch and his unease at the management actions.

What he did blow the whistle on was a coverup by Morton Thiokol of the long trail of engineering dissent over the previous year or so, due mostly to Boisjoly and several colleagues.

It is hard, even in hindsight, to say that Boisjoly himself did not do all he should have done on the eve of the launch, and is therefore criminally liable (I'll agree that his management was at fault). Who could he have gone to with just a few (nighttime) hours before the launch, with no irrefutable evidence, and no support from either his management or from NASA? (It has been suggested that NASA was under pressure from the White House to launch in time for the State of the Union speech that day; Boisjoly wouldn't have found many politicians willing to delay the launch!) In hindsight, most people would agree that he was right to object, but at the time he would have been rather isolated.

I think it is important to stress that Boisjoly (if his own account is trustworthy) was not "turning state's evidence after the fact," but rather blowing the whistle on a coverup of his internal dissent.

-Jeff Mogul

P.S.: This videotape is fascinating and a lot more damning of both NASA and Morton Thiokol than my summary is. It's also quite sad; in the process of urging a room full of MIT students to be prepared to blow whistles, Boisjoly also conveys the strong personal costs of doing so. I'll try to find out how people can obtain a copy.

In "Decent Alarm"? (Re: Mariner 1 or Apollo 11? in RISKS-5.70)

Bruce N. Baker <BNBaker@KL.SRI.COM>
Mon 7 Dec 87 10:46:49-PST

The idea of a "decent alarm" conjures up all sorts of images and fantasies for me, but perhaps Brent Chapman meant "descent alarm".

Bruce

[Skunked again. Thanks for descenting. PGN]

Need for first-person anonymous reporting systems

Eugene Miya <eugene@ames-nas.arpa>
Mon, 7 Dec 87 09:16:59 PST

The Mariner and F4 canopy (not computer related) stories appear to be indicative of certain types of bureaucracies. While I investigate the Mariner story (I have two leads at the moment), I think that it appears to me that normal academic reporting and publication procedures fail us in these matters. Bureaucracies don't like negative subjects to be remembered (almost, I just remembered today is Dec. 7).

If we are ever going to progress out of the software muck, we are going to have to come up with mechanisms to replace all of our ancedotal information with better information. This has to be separate from any type of watch-dog enforcement like "Golden Fleeces," ombudsmen or Inspector Generals. We have to throw out hearsay. Perhaps an anonymous Email system (lots of inherent problems) to a third party? I don't know, but it's something to think about.

--eugene miya

Apollo 11 computer problems

Michael MacKenzie <mm@purdue.edu>
Mon, 7 Dec 87 12:11:57 EST

Exerpt from Apollo, Expeditions to the Moon,
Scientific and Technical Information Office, NASA, Washington D.C., 1975

During the landing of Apollo 11

Michael Collins:

At five minutes into the burn (6000 feet above the surface)
... "Program alarm", barks neil, "Its a 1202", what the hell is that?
I don't have the alarm numbers memorized for my own computer, much less for the LM's I jerk out my checklist and start thumbing through it, but before I can find 1202 Houston say, "Roger, we're GO on that alarm" no problem in other words. My checklist says 1202 is an "executive overflow" meaning simply that the computer has been called upon to do too many things at once and is forced to postpone some of them. A little farther, at just 3000 feet above the surface the computer flashes 1201, another overflow condition, and again the ground is superquick to respond with assurances.

Interconnected ATM networks

<treese@ATHENA.MIT.EDU>
Sun, 6 Dec 87 22:22:52 EST

[Based on an article in the _Boston_Globe_, 12/5/87, p.1]

In Massachusetts now, there is a great deal of competition for ATM networks. BayBanks is by far the largest, and many other banks have joined together

in a network to compete with BayBanks in sheer number of machines. BayBanks recently joined NYCE, a network of ATM's in New York. The Bank of Boston also joined, so now Bank of Boston cards work in BayBanks machines.

When the Globe contacted BayBanks, they refused to acknowledge it until told that the Globe had photographed an editor actually using a Bank of Boston card in a BayBanks machine. Pressed further, a BayBanks spokesperson admitted that it worked, and said that they didn't know NYCE was active yet.

Win Treese
MIT Project Athena

Litigation over an expert system

Gary Chapman <chapman@russell.stanford.edu>
Mon, 7 Dec 87 10:28:51 PST

I am not an attorney, but I worked as a consultant in product liability cases for eight years, and I have some comments on the question posed in RISKS about whether one can sue for damages caused by the use of an expert system.

First, who do you sue? Answer: everybody. As long as the parties mentioned in the case of a financial analyst expert system are individuals or distinct corporate entities, they can be sued and they probably will be. This is why in large product liability cases the defendants can be numerous--in cases involving DES, for example, (the drug, not the encryption system) there are literally hundreds of defendants. There does not even have to be a real legal basis for suing a defendant; it becomes incumbent on the defendant to convince the court that there is no legal basis for the lawsuit in a motion for summary judgment. There are even attorneys who specialize in finding defendants who can be sued--for example, in one case I know about, which involved a high school football player who had been paralyzed from a tackle injury during a game, a special attorney was brought in to find potential defendants, and the plaintiff wound up suing the NCAA, which had drafted the rules for playing football that were used by the plaintiff's school district.

One of the few ways in which a person or a corporation can be guaranteed protection from litigation is an indemnity agreement, or indemnity clause in a contract, which explicitly says that in the event of a lawsuit, one of the contracting parties will pick up the legal defense of the other, including all expenses and all judgments. These are pretty rare.

It is correct to assume that a disclaimer, or a warning, or a "terms of agreement" document such as is commonly found in software packages, is no protection against a lawsuit or a judgment against the developer. It is up to a judge or jury to decide whether the warning was adequate, whether it was relevant to the damages, and even whether it was presented to the user in a way that was likely to have actually "warned" the consumer about the use which produced the damages. For example, in a couple of cases I worked on, the plaintiffs brought in a psychologist who specialized in the visual impact of signs--she consulted with municipal transportation systems on how to design signs on subways that would get across essential information, for example.

This psychologist would frequently testify that a warning on a product was ineffective because of the way it was packaged or designed. It is hard to estimate the effect of her testimony on a jury--sometimes the plaintiff won, sometimes the defense won. But this is an illustration of what one is likely to be up against in a case involving large damages.

In another illustration, it often comes up in product liability cases involving drugs that the warnings issued by drug companies and published in a standard reference work called the Physicians' Drug Reference, or PDR, are so dense and so full of information that they no longer convey a "warning" that is intelligible to anyone. Nevertheless, if the drug companies fail to include any particular bit of information then they may be liable for failing to provide a warning for something they knew about.

A jury may award a defendant a judgment even when there was a warning or a terms of agreement document. The defendant may then appeal the judgment based on a claim that the defendant did everything in his power to avoid the damages--for example, a lawn mower company put a big, nasty looking warning on some part of the lawn mower that said don't do such and such because you may get your hand caught in there and lose some fingers, but the plaintiff did it anyway and for some reason the jury decided he should get some money from the defendant. But appeals are expensive, and it's likely that the defendant and the plaintiff will settle the case for some dollar figure, and perhaps the money will be paid by an insurance company. There is not much one can do to predict what a jury will decide, even in the most straightforward cases. I remember asking one juror why she voted the way she did, and she said that she understood that she was supposed to give *someone* some money, and she thought the defendant could pay more than the plaintiff could. A jury may also decide that a warning could have been better, but that the plaintiff was also at least partially responsible for his injury through "contributory negligence," so the dollar amount of the judgment may be lower because of this.

In California, where I live, there is a goofy law that if one of the defendants in a multi-party suit is judged to have been responsible in any way, that defendant is liable for the percentage of responsibility, no matter how small. In other words, if the jury decides that defendant A is 99% responsible, and defendant B is only 1% responsible, and the judgment is $10 million, defendant B has to pay the plaintiff $100,000.

I don't know of any cases of product liability involving damages alleged to have occured because of the use of an expert system, but the law is likely to be the same for such cases as it is for any other product liability case.

LEICHTER-JERRY@CS.YALE.EDU <"Jerry Leichter>
Mon, 7 Dec 87 10:53 EST

<LEICHTER@VENUS.YCC.YALE.EDU>
Subject: re: Can you sue an expert system
To: risks@csl.sri.com

In RISKS-5.69, Barry Stevens becomes another in a long line of people to raise

the question "If an expert system gives bad advice, who can I sue?" I find it extremely disturbing that this is considered an interesting question by ANYONE, let alone by technically sophisticated people. It is a symptom of the pervasiveness of our misplaced trust in buzzwords and, more generally, in computers: If the computer said it, it MUST be right.

We have no idea how to build an expert system with anything you would want to call "understanding" or "responsibility" - or even "intelligence" - in any but the most narrow sense. There is no indication that we will be able to build such a system any time soon. An expert system is a clever way of encoding a textbook and some guidelines. If well designed, it happens to be a lot easier to use than the typical textbook - but then again there are good textbooks and poor textbooks. It should make no more sense to sue an expert system than it does to sue a textbook. It should make no more sense to sue a vendor of expert systems than it does to sue a publisher or a bookstore because of inaccurate information in one of the books they sell. It should make no more sense to sue the "knowledge engineer" who did the fairly routine work of organizing data from a group of experts into an expert system than it would to sue an editor of an encyclopedia. Finally, it should make no more sense to sue the expert who contributed to an expert system than it does to sue the author of an encyclopedia article.

As a general rule, it's almost impossible to sue someone for advice offered in a book. You need a much closer relationship with the expert - the expert has to hold himself up not just as an expert "in general", but as an expert in your particular problem. In paying for him to work on your particular problem, you are creating expectations and obligations that go far beyond what you can expect from an author of a book.

In our litigious society, someone WILL sue over the advice given by an expert system. They'll sue everyone they can. They may even win, eventually. If they do it will be a sign that enough advertising, enough magazine articles, enough speeches on how "intelligent" expert systems are have been given that the courts have decided that people are legimately entitled to view this claim as more than mere "seller's talk". The first such case to be upheld is likely to see the death of the expert systems business: We do not know how to build expert systems that can come close to living up to the expectations being raised for them. No one will be able to afford the resulting liabilities. From my point of view, if it ever came to that, it would be a result richly deserved by an industry that has lived on hype. What disturbs me is that it's unlikely the legal system, should it ever start on this path, will draw quite the distinctions we in the business draw between expert systems and other kinds of applications. Would you like to be personally liable because the database program you wrote didn't deal with spelling errors and as a result someone missed an incorrectly-typed reference in an on-line catalog and was somehow injured as a result?

There is SO much hype about computers and their miraculous powers, and SO much of a willingness to believe it on the part of the public, that I think we as professionals have an obligation to tell people, at every opportunity, just how limited our real abilities are, and are likely to remain in the forseeable future. Speculations about the legal liabilities of AI's are fine as philosophy, but as anything more than speculation about possible futures, they are uninformed about either the technical or legal realities. If they lead people

to place their trust in such systems inappropriately, then can be downright dangerous.

-- Jerry

Re: Can you sue an expert system?

<"Bruce_Hamilton.OsbuSouth"@Xerox.COM>
7 Dec 87 11:49:47 PST (Monday)

No new law needed here. I'm a layman, not a legal scholar, but it seems to me that an "expert system" is precisely analogous to a book. The only difference with a book is that you have to do all the "if-then" calculations yourself ("if your net worth according to this formula is > X, then turn to page Y...").

Bruce

What this country needs is a good nickel chroot (Re: RISKS-5.63)

Bob English <lcc.bob@SEAS.UCLA.EDU>
Mon, 30 Nov 87 12:33:02 PST

> From: "Joseph G. Keane" <jk3k+@andrew.cmu.edu>
> Subject: Re: "UNIX setuid stupidity" (RISKS-5.57)
> The designers of UNIX considered that a trusted program may wish to allow
> operations only on a certain part of the directory tree. So they provided
> the `chroot' system call, ... --Joe

Chroot doesn't work very well. Since the super-user can create device inodes, it can access or modify any disk area, regardless of the limitations enforced by the new root. 'Chroot', by itself, will not prevent a determined invader from penetrating to the rest of the system. It does, however, prevent penetrations based solely on moving through ".."

--bob--

[To those of you who contributed on this topic, I STILL have a backlog of messages waiting for me to sort out the wheat from the chaff. PGN]

Search RISKS using swish-e

THE RISKS DIGEST

Forum on Risks to the Public in Computers and Related Systems

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

Volume 5: Issue 72

Saturday, 12 December 1987

Contents

`Risks to the Rodent Public in the Use of Computers'

Peter Ladkin <ladkin@kestrel.ARPA>
Fri, 11 Dec 87 11:18:20 PDT

Stray Rodent Halts Nasdaq Computers, by Kenneth N. Gilpin
NYT Thursday, Dec 10, 1987, p.33

An adventurous squirrel touched off a power failure in Trumbull, Conn.,
that shut down the National Association of Securities Dealers'

automatic quotation service for 82 minutes yesterday.
A Nasdaq official estimated that the power failure might have kept slightly more than 20 million shares from being traded. [.....]
The breakdown was also felt at stock exchanges around the country on which options on over-the-counter issues are traded
Power in the Trumbull area, where Nasdaq's main computer center is situated, was restored by the United Illuminating Company shortly after the squirrel lost its life - and Nasdaq its power - at 10:43 A.M.
But a power surge that accompanied the utility's resumption of service disabled Nasdaq's mainframe computers and seriously damaged the electrical system at the complex, making it impossible to use backup generators.
Nasdaq officials then switched to a backup computer system in Rockville, Md. By 12:05 P.M., service had been partly restored. Full service was available by 2:30 [the Nasdaq official] said . [.....]

Well, I guess a martyr to one segment of the mammal population is a scapegoat to another. The disruption could have been more serious if more people hadn't squirrelled away their savings after black monday.

peter ladkin

Yet another virus program announcement fyi

Martin Minow ML3-5/U26 223-9922 <minow%thundr.DEC@decwrl.dec.com>
11 Dec 87 11:55

From CRTNET, number 115. From T3B%PSUVM.BITNET.

Subject: Christmas Virus Warning

If you are at a CMS site and receive a program called CHRISTMA EXEC, please (a) warn your postmaster and (b) discard the exec (or keep a copy for the postmaster to look at, but DO NOT RUN IT). This exec paints a Christmas tree on your screen and then sends itself to everyone named in either your NAMES or NETLOG files. The result is potentially serious stress on Bitnet and on your local spool system, and possibly a few system crashes here and there as the number of reader files soars and exceeds the maximum. The Christmas tree isn't all that pretty, and the joke is pretty mean.

A word to the wise. Your postmaster will thank you. Michael Sperberg-McQueen

---

IBM invaded by a Christmas virus

Dave Curry <davy@intrepid.ecn.purdue.edu>
Sat, 12 Dec 87 10:02:24 EST

(From the Lafayette (Indiana) Journal & Courier, December 12, 1987. Quoted without permission.)

IBM Woes -- Computerized grinch jams the mail

BINGHAMTON, N.Y.- A computerized Grinch invaded IBM's electronic mail Friday.

An illegal software-style so-called Christmas card sent through IBM's electronic mail jammed desk-top computer terminals, spokesman Joseph E. Dahm said.

The so-called virus program forced plant officials to turn off internal links between computer terminals and mainframe systems to purge the message, Dahm said.

IBM sources say the link was off from 45 minutes to 90 minutes depending on the location.

The program is known as a virus because it enters computer programs and replicates itself automatically.

Curious employees who read the message titles "Christmas" in the morning electronic mail discovered an illustration of a Christmas tree with "Holiday Greetings" superimposed on it. A caption advised "Don't browse it, it's more fun to run it."

"That was the hook," an IBM source said. "A lot of people thought they could take a peek and then kill the message, but once opened, it was too late."

The program automatically entered a security log listing contacts made from the individual computer terminal, duplicated and mailed itself to new victims.

Like a Pandora's Box, once opened, the program rarely accepted commands to stop, sources said. Operators who turned off their terminals to stop the Christmas message lost electronic mail or unfinished reports not filed in the computer.

This article seems to have a lot of things in it that the reporter didn't understand. I assume that the "terminals" in question are really PC's connected to the mainframes; for one thing. Plus, I presume the "Don't browse it" refers to the VM/CMS "BROWSE" command used for looking through files, and not just to the regular English word.

Does anyone have any more info from a source which understands all the big words?

--Dave Curry, Purdue University

Virus Protection Strategies

Joe Dellinger <joe@hanauma.STANFORD.EDU>
Wed, 9 Dec 87 02:22:36 pst

From recent postings it sounds like Personal Computer viruses are getting to be a problem. In 1982 when I wrote my Virus, nobody I knew thought such things could even exist. When I explained what I had made to fellow hacker types, the usual reaction was "What a wonderful idea! But an innocuous virus is boring. I want to create an EVIL one...". Given this reaction, and the increasing knowledge of how such things work, I would expect the number of viruses to increase.

What strategies can we use to protect ourselves? Best, of course, is to make it impossible. Make the DOS area on the disk read only. Put DOS

in rom on the machine. Write protect as many disks in your collection as feasible. Make sure write protection is done in hardware.

Whenever a new disk is used for the first time, compare the DOS on that disk with the DOS in memory. If they don't match, issue a warning. Make a program that performs such a check a standard utility.

The best solution, I think, is to simply make writing a Virus difficult. Don't leave any convenient holes in DOS where a Virus can hide out. Have many places in the boot process where parity checks on pieces of DOS are done. Have unused bytes scattered here and there in DOS that are different in every copy of DOS sold. Have code in ROM that performs some sort of verification before booting a disk. Have several different versions of this ROM in use, sensitive to different things, so that you can't assume a virus that works on your machine will also work on all machines. Use self-modifying code in the boot process. Have several different ways that DOS can be layed out on the disk, and pick a random one at initialization time.

While none of these schemes would make a Virus impossible, any of them would make creating one very tedious. I think the only reason we aren't experiencing a plague of viruses already is that it is a fair amount of work to create one. It is also a lot more work to create a "careful" virus than it is to create a "careless" one. Most of the viruses I have heard of are not purposefully evil, they just don't bother to check that they aren't accidentally damaging something.

Rich Kulawiec <rsk@s.cc.purdue.edu>
Thu, 10 Dec 87 21:37:57 EST

postmaster@decwrl.dec.com
Subject: New chain letter running around internet/usenet

Yes, there's another chain letter running around out there. We've just wiped out a few hundred local copies, and it looks like it got here after bouncing around a DECnet site somewhere. The oldest letter in the chain is from 'DECWSE::ROST "Randi Rost"' but of course I've no idea if that's the original point of origin. There's no telling how much mail spooler space or xmit time is being chewed up by this @($#*&!@ letter, of course; but I figured I'll tell y'all...well, those of you that didn't already know the good news.

Rich

[Enormous sequential history of the chain letter deleted... PGN]

On-line bank credit cards

John R. Levine <johnl@ima.ISC.COM>
Tue, 8 Dec 87 22:06:30 EST

In a recent job, I was involved in processing Master Card and Visa credit

card charges, and it seems to me that their automated processing system is enormously vulnerable to fraud. Let me explain how it works.

We were taking a lot of credit card orders over the phone, and had all of the order information in a data base. It seemed like a bad idea to print out zillions of charge slips, so I investigated submitting the charges on-line. It turned out to be unbelievably easy.

Readers are doubtless familiar with the verification terminals found next to cash registers, into which a clerk puts the card, keys in the amount of the sale, it calls in and comes back with an approval code or denial message. It turns out that the terminals can do considerably more than that. They can post charges to a customer's bill, making it unnecessary to physically send in a slip, and can also post refunds. Many stores use an "auth/post" transaction which authorizes and posts a charge in a single operation while you wait. When the terminal runs the transaction, it calls a local concentrator which sends the request to the Giant Bank Computer in Omaha, which in turns sends the request to the cardholder's bank, with the bank sending back the response. The authorization code the merchant writes on the check comes from the cardholder's bank. I've watched while requests for European cards ran, and they take only a few more seconds than usual. It's pretty impressive. Funds from transactions posted by 7:00 PM each day are supposed to be available in the merchant's bank account the next morning. The Giant Bank Computer sends a printed log of posting transactions which usually arrives about a week after the actual transaction. Each call that posts anything produces a separate log page. The bank, by the way, thinks this is all great since they are spared all of the physical work of processing the charges, and charged us about half what they would have had we sent in slips.

The protocol between the authorization terminal and the concentrator is unencrypted 300 baud ASCII. It took me about a day to write a program for a PC that implemented the protocol and that we used to process our thousands of credit card sales via auth/post transactions. The terminal calls in, and after the concentrator answers it sends a record consisting of the merchant's account number, the customer's account number, the amount to charge, and a code indicating what kind of transaction to perform. The response is the actual string displayed on the transaction terminal, e.g. "AUTHORIZED: 123456". The messages in each direction are protected by a simple one-byte checksum, with messages with bad checksums being ignored. There is no log-on or log-off protocol; the terminal calls up, sends and recieves as many transactions as it wants, and then hangs up.

The first problem is that there is no protection against duplicated transactions when a message is thrown away due to a bad checksum. We had a few, most of which we fortunately noticed and fixed before the customer got the bill, and would probably have had many more had the concentrator not been physically very close on a clean phone line. More importantly, this scheme seems awfully easy to spoof. Merchant numbers are usually printed next to the merchant's name on a charge slip. Card numbers are all over the place. For example, imagine that I just bought something at a store that runs a slip, then does an auth/post on its terminal and then just files the slip. (I know lots of stores that do that.) I then run home and call up from my PC, sending a refund transaction for the same

amount and merchant number. The merchant probably would never notice the refund in the blizzard of paper that comes from the Giant Bank Computer, or if it did, would probably assume that it was a voided sale or accidental overcharge. Another less subtle risk is that were someone to sabotage the Giant Bank Computer, as far as I can tell all bank card charges would stop. I'm sure they have good physical security and backups, but even a day or two of downtime could cause major trouble for a lot of merchants.

We probably have yet another case here of banks using security through obscurity (which is why I'm certainly not going to go into any more detail about the protocols.) I've heard that they are very touchy about people discussing the checksum algorithm used in credit card numbers, even though the algorithm is printed in the ANSI standard for financial transaction cards. The online transaction scheme is, to put it mildly, a much greater exposure.

American Express was much less willing to automate the procedure -- they were happy to do on-line authorizations through the same simulated transaction terminal. We still had to send in physical charge slips. I thought they were just being obnoxious, but upon reflection, I can see that they may have had their reasons.

John Levine, johnl@ima.isc.com or ima!johnl or Levine@YALE.something

---

Central Locking

Martyn Thomas <mcvax!praxis!mct@uunet.UU.NET>
Tue, 8 Dec 87 12:09:10 BST

A colleague's BMW 525e developed a disturbing fault. After we had returned to it on several occasions to find all the doors unlocked, we set a trap. After parking it, we locked the doors, went 20 yards away and waited. Five minutes later, we heard the central 'locking' system unlock all the doors.

The fault was traced to a loose wire.

Martyn Thomas, Praxis plc, 20 Manvers Street, Bath BA1 1PX UK.
Tel: +44-225-444700. Email: ...!uunet!mcvax!ukc!praxis!mct

Product Liability

Martyn Thomas <mcvax!praxis!mct@uunet.UU.NET>
Tue, 8 Dec 87 12:25:07 BST

An EEC Directive, mandatory throughout the Community from Summer 1988, imposes strict (ie no-fault) liability on manufacturers of products which cause personal injury or damage to personal property as a result of a manufacturing defect. For imported goods, the original importer into the EEC is liable.

Liability is strict: the purpose of the Directive is to ensure that injured people can recover damages without having to prove negligence (usually impossible and always expensive).

The UK has enacted the Directive as Part 1 of the Comsumer Protection Act 1987 (which comes into force on March 1st 1988). The UK has included a defence: "that the state of scientific and technical knowledge at the relevant time was not such that a producer of products of the same description as the product in question might be expected to have discovered the defect if it had existed in his products while they were under his control". This defence is not allowed in France, the Netherlands, or Luxembourg. West Germany allows the defence except for Pharmaceutical products.

It is expected that the Act will greatly increase the adoption of software Quality Assurance (to conform to ISO standard ISO 9001) and the use of mathematically rigorous specification and development methods (VDM, Z etc).

Martyn Thomas, Praxis plc, 20 Manvers Street, Bath BA1 1PX UK.
Tel: +44-225-444700. Email: ...!uunet!mcvax!ukc!praxis!mct

Wishing the deceased a merry christmas (automatically)

Bill Lee <munnari!phadfa.adfa.oz.au!lee@uunet.UU.NET>

Text in << <> was lifted without permission from the "Sydney Morning Herald" Friday Dec. 11 1987

> << The Advance Bank sent a Christmas letter to a Manly account holder. It read: "Dear Valued Customer, On behalf of your local branch team, may I wish you a very safe and happy Christmas 1987, and a prosperous 1988." The man died earlier this year - and the bank recognised this by addressing the letter to Mr Arthur .... Decd. <>

An example (presumably) of blindly asking a computer to print out one christmas letter for each human customer (as against company or corporate entity) without first checking to see if the person is still thought to be alive (by the absence of contary notice, such as a death certificate sent to the bank to allow access to the deceased's account). The Bank did receive notice, otherwise they would not have marked it to be sent to a person "Decd."

Mail: Bill Lee, Dept. Electrical & Electronic Engineering, University College, UNSW, ADFA, Canberra. 2600. Phone: (062) 68 8193, Telex: ADFADM AA62030, ACSNET: "bill@eeadfa.ee.adfa.oz"

Air Traffic Control Computer Replacement Schedule

Dan Ball <ball@mitre.arpa>
Thu, 10 Dec 87 10:09:26 EST

In RISKS 5.67 (01 Dec 87), Rodney Hoffman indicated that news accounts concerning the recent failure of the 9020 computer at the Los Angeles Center made no mention of a date for installation of a replacement computer system.

For your information, the replacement system has been installed at Los Angeles and is scheduled to be fully operational by March 01, 1988. The replacement program has been proceeding ahead of schedule, with replacement computers operational at about one-third of the centers. All sites are scheduled to be operational by June of 1988.

The 9020 computers are being replaced with dual redundant IBM 3083 processors which will rehost the existing applications software. Reports from the field indicate that the reliability of the new systems is significantly better than that of the 9020 as a result of the new hardware and improvements in the operating system.

However, the new computers are running 18-year-old software, and the display channel computer will not be replaced until the Advanced Automation System is introduced in the next decade, so it may still be necessary occasionally to shift to the less capable backup system, hopefully much less frequently.

Re: United Airlines O'Hare Sabotage?

<Mills@UDEL.EDU>
Thu, 10 Dec 87 10:26:29 EST

There was a famous incident at an AT&T CO in Manhattan many years ago when a fire destroyed much of the office. The rebuilding program was so intricate and extensive that it was written up in a technical journal. Recently a similar thing happened in Brooklyn, but I don't have the details. I was told at a NAS meeting yesterday that AT&T has a videotape documenting the rebuilding effort. Apparently, most of the effort goes into re-coppering and re-framing the loops. I would guess that extensive use of highly multiplexed glass might make such rebuilding much easier. Maybe the increase in robustness in the face of massive destruction of CO facilities will balance the vulerability to backhoe attack.

Dave

Search RISKS using swish-e

THE RISKS DIGEST

Forum on Risks to the Public in Computers and Related Systems

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

Volume 5: Issue 73

Sunday, 13 December 1987

Contents

Australian datacom blackout

Barry Nelson <bnelson@ccb.bbn.com>
Tue, 8 Dec 87 16:11:43 EST

From The Australian, 23 November 1987, Sydney, Australia, Page 1, 2nd edition.
[without permission]

8-Column BANNER: SABOTEUR TRIED TO BLACK OUT AUSTRALIA

The heart of Sydney's business district remains in chaos after a dangerously

well-informed saboteur wreaked havoc on the city's fragile telecommunications system in an attack intended to destroy [Australian] Telecom's operations nationwide. [An estimated 2000 central city services remain out this morning]

Investigators described the sinister saboteur as a lone, former Telecom employee with expert knowledge of the underground cables network.

[...] But Telecom said it could have been much worse. [only Sydney was hit] but all international services are routed through Sydney [...]

[The attacker entered the underground tunnels and] severed 24 of the 600 heavy cables in 10 carefully selected locations. The bizarre attack knocked out 35,000 telephone lines in 40 Sydney suburbs and brought dozens of [ATMs, POS, stores, telex, facsimile and betting office] services to a standstill. [...]

Hundreds of computers broke down, leaving communications and computer specialists to ponder the real possibility of vital information being erased from tapes in banking, insurance and other industries.

[The largest banks and the international and local PTT offices were all cut off. Speculation is that the attacker's information was over two years old because the same attack at that time would have completely crippled Telecom Australia. Security locks have now been put on the manhole covers. Just the reconnection effort is estimated to cost millions of dollars and full damages will not be known until businesses have time to detect losses. A man seen leaving a manhole on Wednesday night was possibly the saboteur reconnoitering his targets. ...]

Page 2, 4-columns, 5x7 foto - SABOTAGE IS A NIGHTMARE FOR TELECOM'S WEARY BAND

Four hundred Telecom managers, technicians and linesmen worked frantically toward today's 9am deadline [to restore the damaged services. Some worked 48 hours straight with only brief napping.]

When the enormity of the sabotage was realised (sic) on Friday, a team of technicians and linesmen was sent into the tunnels to discover the damage. The cuts, which were only a centimeter across, could only be found by touch in the dark, dank tunnels.

"The workmen had to run their hands along the entire length of the cables until all the cuts were discovered. Some of them walked over 20 miles on Friday night", said Roger Bamber, the [New South Wales] Telecom Operations Manager [The system contains 27 km of tunnels. It is estimated that the damage could have been done by one well-prepared man over a period of less than one hour.]

Things started to go wrong in the city about 7pm on Friday, and workmen searched through the night until 6am to find all the damage. [Other searches were launched over half the state for bombs or other evidence of sabotage.]

[... in other articles]

[Employees' anger at turncoat Telecom policies suggest an insider hacked the cables. The telephone workers' union objects to deregulation which has

resulted in years of acrimonious debate. Last week's Telecom statements suggested that an independent regulator will be created. The union doesn't approve of this action and prefers monopoly.]

-----One must wonder if the REAL crime was obscured by the Telecom outage-----

---

Finally, a primary source on Mariner 1

John Gilmore <hoptoad.UUCP!gnu@cgl.ucsf.edu>
Sun, 13 Dec 87 05:30:10 PST

My friend Ted Flinn at NASA (flinn@toad.com) dug up this reference to the Mariner 1 disaster, in a NASA publication SP-480, "Far Travelers -- The Exploring Machines", by Oran W. Nicks, NASA, 1985. "For sale by the Superintendent of Documents, US Government Printing Office, Wash DC." Nicks was Director of Lunar and Planetary Programs for NASA at the time. The first chapter, entitled "For Want of a Hyphen", explains:

"We had witnessed the first launch from Cape Canaveral of a spacecraft that was directed toward another planet. The target was Venus, and the spacecraft blown up by a range safety officer was Mariner 1, fated to ride aboard an Atlas/Agena that wobbled astray, potentially endangering shipping lanes and human lives."

..."A short time later there was a briefing for reporters; all that could be said -- all that was definitely known -- was that the launch vehicle had strayed from its course for an unknown reason and had been blown up by a range safety officer doing his prescribed duty."

"Engineers who analyzed the telemetry records soon discovered that two separate faults had interacted fatally to do in our friend that disheartening night. The guidance antenna on the Atlas performed poorly, below specifications. When the signal received by the rocket became weak and noisy, the rocket lost its lock on the ground guidance signal that supplied steering commands. The possibility had been foreseen; in the event that radio guidance was lost the internal guidance computer was supposed to reject the spurious signals from the faulty antenna and proceed on its stored program, which would probably have resulted in a successful launch. However, at this point a second fault took effect. Somehow a hyphen had been dropped from the guidance program loaded aboard the computer, allowing the flawed signals to command the rocket to veer left and nose down. The hyphen had been missing on previous successful flights of the Atlas, but that portion of the equation had not been needed since there was no radio guidance failure. Suffice it to say, the first U.S. attempt at interplanetary flight failed for want of a hyphen."

Mariner 1 from NASA reports

Doug Mink <mink%cfa@harvard.harvard.edu>

Tue, 8 Dec 87 11:42:36 EST

JPL's Mariner Venus Final Project Report (NASA SP-59, 1965)
gives a chronology of the final minutes of Mariner 1 on page 87:

4:21.23 Liftoff
4:25 Unscheduled yaw-lift maneuver
"...steering commands were being supplied, but faulty application of the guidance equations was taking the vehicle far off course."
4:26:16 Vehicle destroyed by range safety officer 6 seconds before separation of Atlas and Agena would have made this impossible.

In this report, there is no detail of exactly what went wrong, but "faulty application of the guidance equations" definitely points to computer error. "Astronautical and Aeronautical Events of 1962," is a report of NASA to the House Committee on Science and Astronautics made on June 12, 1963. It contains a chronological list of all events related to NASA's areas of interest. On page 131, in the entry for July 27, 1962, it states:

> NASA-JPL-USAF Mariner R-1 Post-Flight Review Board determined that the omission of a hyphen in coded computer instructions transmitted incorrect guidance signals to Mariner spacecraft boosted by two-stage Atlas-Agena from Cape Canaveral on July 21. Omission of hyphen in data editing caused computer to swing automatically into a series of unnecessary course correction signals which threw spacecraft off course so that it had to be destroyed.

So it was a hyphen, after all. The review board report was followed by a Congressional hearing on July 31, 1962 (ibid., p.133):

> In testimony befre House Science and Astronautics Committee, Richard B. Morrison, NASA's Launch Vehicles Director, testified that an error in computer equations for Venus probe launch of Mariner R-1 space-craft on July 21 led to its destruction when it veered off course.

Note that an internal review was called AND reached a conclusion SIX DAYS after the mission was terminated. I haven't had time to look up Morrison's testimony in the Congressional Record, but I would expect more detail there. The speed with which an interagency group could be put together to solve the problem so a second launch could be made before the 45-day window expired and the lack of speed with which more recent problems (not just the Challenger, but the Titan, Atlas, and Ariane problems of 1986 says something about 1) how risks were accepted in the 60's, 2) growth in complexity of space-bound hardware and software, and/or 3) growth of the bureaucracy, each member of which is trying to avoid taking the blame. It may be that the person who made the keypunch error (the hyphen for minus theory sounds reasonable) was fired, but the summary reports I found indicated that the spacecraft loss was accepted as part of the cost of space exploration.

Doug Mink, Harvard-Smithsonian Center for Astrophysics, Cambridge, MA
Internet: mink@cfa.harvard.edu
UUCP: {ihnp4|seismo}!harvard!cfa!mink

Mariner I

"Marty Moore" <mooremj@aim.rutgers.edu>
11 Dec 87 16:54:00 EST

I've just caught up on two months of back RISKS issues. I have the following to contribute on Mariner I, based on my time at the Cape:

1. Mariner I was before my time, but I was told the story by a mathematician who had been at the Cape since 1960. According to him, an algorithm, written as mathematical formulae, involved a Boolean entity R. At the point of failure, the mathematician had written NOT-R, that is, "R" with a bar above the character; however, the programmer implementing the algorithm overlooked the bar, and so used R when he should have used NOT-R. This explanation could subesequently have been interpreted as "missing hyphen", "missing NOT", or "data entry problem", all of which we've seen in recent contributions.

2. I think the FORTRAN version of the story is very unlikely. Remember that the error occurred in a critical on-board computer. I consider it extremely unlikely that such a computer would have been programmed in FORTRAN in 1962, considering that the first use I saw of FORTRAN in a ground-based critical system at the Cape was not until 1978! (Of course, I wasn't aware of *every* computer in use, so there may have been an earlier use of FORTRAN, but I'd be surprised if it was more than a few years earlier.) It is possible that the originator of the FORTRAN version of the story may have been aware of another error caused by the period/comma substitution, and also aware of the Mariner problem as a "single character" error, and incorrectly associated the two.

> [There were other messages (e.g., from Eric Roberts, Eugene Miya, and Jim Valerio) on this subject as well, but there is too much redundancy or lack of definitude to include them all... PGN]

Re: Computer-controlled train runs red light

Nancy Leveson <nancy@commerce.UCI.EDU>
Sat, 12 Dec 87 20:31:44 -0800

In Risks 5.69, Steve Nuchia writes:

> >Surely these engineers can't be so paranoid as to think that an exact
> >duplication of their (primarily digital) relay-based control system in
> >software would be hard to verify. It should at least be possible to build a
> >software implementation that could be easily shown to be equivalent to the
> >relays, leaving aside the problem of validating an arbitrary "spagetti code"
> >implementation.

The failure modes of mechanical systems are usually well understood and very limited in number. Therefore, system safety engineers are able to build in interlocks and other safety devices to control these hazards. The failure modes of software are much more complex and less is known about how to control software hazards. Even if the same functionality

is implemented in the software, that does not mean that the failure modes and mechanisms are identical nor that the complexity of the two systems is equivalent. Software also exhibits discontinuities not usually found in mechanical relay systems.

If identical function is implemented in software, then the probability of requirements errors in the software is equivalent to design errors in the mechanical system. But there is an additional possibility of introducing implementation errors in the software. Given identical function of both types of systems (and thus identical probability of accidents arising from problems in this functional design), then the additional probability of design and coding errors in the software is not necessarily identical to the probability of random "wearout" failures in the mechanical system (the primary cause of failures in mechanical systems).

> >Automobile traffic light control boxes, based on relay technology quite
> >similar to that used in railroads, fail every so often due to ants building
> >mounds in the nice warm cabinets. People have been killed by this bug in a
> >relay system, yet it fails to generate the kind of emotional response that
> >software bugs do. ---

Certainly there are accidents in conventional mechanical systems. However, the concern about software bugs is more than just an irrational emotional response. There are very good scientific reasons for it. Besides that noted above (greater understanding of failure modes and mechanisms in mechanical systems and thus better methods to control hazards), it is also possible to perform risk assessment on mechanical systems due to reuse of standard components with historical failure probability data. This is not possible for software. Certainly these risk figures are not always accurate, but it is not irrational to feel more comfortable about a system with a calculated risk of an accident of 10^-9 over 10 years time than a system with a calculated risk of "?".

Besides, I question whether accidents caused by mechanical failures generate less emotional response than accidents caused by software bugs. Consider Challenger and Three Mile Island. It is natural for computer scientists to have considerable interest in computer-related accidents and reasonable for non-computer scientists to be worried about software bugs.

Nancy Leveson, UCI

Re: interconnected ATM networks

John R. Levine <johnl@ima.ISC.COM>
Tue, 8 Dec 87 22:06:27 EST

The story about BayBanks vs. Bank of Boston ATM cards is even more interesting than it initially sounds. BayBanks and Bank of Boston are arch-rivals in consumer banking, and they run the two largest ATM networks in the region, XPress 24 and Yankee 24, respectively. (Yankee 24 is a consortium, but Bank of Boston is by far the largest participating bank.) When Yankee 24 was expanded from its Connecticut base to cover all of New England, XPress 24 was invited to join, but they declined and BayBanks has since filed an anti-trust suit against

Yankee 24, so far to no effect.

A few years ago, the two banks jointly set up a system of retail store cash dispensers called Money Supply. Both XPress 24 cards and Monec cards (Bank of Boston's previous network, now folded into Yankee 24) work at Money Supply machines. One day shortly after Money Supply came up, while waiting for a plane at Logan Airport in Boston, I noticed that one of the BayBank XPress 24 machines had a small Money Supply sticker on it, and upon trying my Bank of Boston card, was surprised to discover that it worked. Subsequent experimentation showed that other than the four airport BayBank machines, neither bank's machines accepted the other's cards, and the XPress 24 machines gave a peculiar message that "your bank has restricted use of this card at this terminal." The fact that Bank of Boston cards worked at the airport was not widely known, even at the two banks.

Thus I was as surprised as anybody to discover that when both banks joined NYCE, they started taking each other's cards, since I was under the impression that BayBanks' network already routed Bank of Boston requests via other paths which were usually blocked, and vice versa.

This suggests that perhaps BayBanks doesn't entirely understand how their ATM network routes messages to off-network banks. If I were they, I'd be pretty nervous.

John Levine, johnl@ima.isc.com or ima!johnl or Levine@YALE.something

---

Re: ATM PIN numbers

<new@UDEL.EDU>
Sun, 29 Nov 87 21:40:17 -0500

For what it is worth, the PINs for Mellon cards are not stored on the cards. I had both a checking and a savings account at Mellon. Several years after opening them, I closed the checking account but retained the savings account. All of a sudden, the card no longer worked. I visited a branch office in person to find out what happened. It seems that when the checking account closed, the first digit of the PIN number changed. The clerk implied that I had simply forgotten what the number was, but this was not the case; I had been using the number for years. I suspect that the data entry person who closed the account bumped the wrong key on the screen form, accidently changing the PIN field. I never followed it further. However, since the card was never out of my possession, I know that the PIN is not on the card.

With regard to Otto Makela's "Your bank's computer is down" message appearing after entering the PIN: I suspect that all of your information is gathered before any connection to your bank is attempted. This prevents tying up the lines during "think time". I think the X.25 standards even include a special kind of "open connection" packet, whereby an encrypted batch of data is sent off and a yes/no reply comes back without any true "connection" ever being established. Of course, this does not invalidate any of his points, nor does it imply that other countries or banks follow the same protocols as Mellon Bank, USA.

Darren New

[For the record, there were somewhat overlapping messages from John McLeod, Robert Stroud, B.J. Herbison, and Peter da Silva. PGN]

Control-tower fires

<dvk@SEI.CMU.EDU>
Wed, 9 Dec 87 10:28:01 EST

Control-tower fire - a nightmare that wasn't...

I was flying out of Cairo airport in 1982 or so, and the night before they had had a control tower fire. The immediately visible ramifications of this were that none of the terminal monitors (the flip chart kind you see in European train stations) were working, and the gate agents reported delays on almost every outbound flight (I am not sure about inbound flights - I got to the airport at 6:45am (for a 10:30am flight) so there was not much inbound).

Cairo International is a fairly busy aiport, yet most of the flights were departing within an hour of scheduled departure time (i.e., they were "on time" for Cairo). The reason for this is that they had ATCs in the burned out shell of the control tower visually sighting aircraft on the ground (and possibly in the air), communicating via walkie-talkies to the aircraft and to ground based directors who literally waved the planes onto the runways.

Basically, everything worked. Why? Because the airport was able to shift into a manual mode of operation when the tower (and computers?) were down. There were no super failsafes to get in the way. Now, I am not advocating the removal of failsafes. What I am suggesting is that our current failsafes be made a little less restrictive. In Chuck Weinstock's post about O'Hare, the aircraft had trouble getting fuel because of safety interlocks, even when technicians *knew* there was no danger to the fuel feed. In Cairo, the whole system was toasted, but it kept running. Granted, there are differences, but there are also lessons to be learned here. Failsafes whould keep you from making stupid mistakes, but not prevent you from making intelligent decisions.

Loss-of-orbiter (Re: RISKS DIGEST 5.70)

Dani Eder <ucbcad!ames.UUCP!uw-beaver!ssc-vax!eder@ucbvax.Berkeley.EDU>
Tue, 8 Dec 87 11:39:44 pst

Reliability work done here at Boeing (as part of the Advanced Launch System program) predicts the loss-of-orbiter rate to be 1 in 60 launches AFTER the fixes in progress are completed. The loss of crew rate is somewhat lower, since there are accidents where you render an Orbiter unuseable, but do not kill the crew. For example, landing hard can stress the structure enough that it would be unsafe to ever fly again, but with no visible damage occurring.

What our reliability work indicates, is that adoption of airplane-like design rules: such as ability to fly a mission with a single engine failure, all engines running before launch, double and triple redundant flight control

systems, and powered (jet engine) return to a runway for the booster stage, should bring the loss-of-payload for a next generation rocket to 1 in 5000 flights.

The lesson we learned from the commercial airplane side of the company is: use improved technology (such as lighter structural materials and smaller electronics) to get better reliability rather than a few more pounds of performance. Your hardware will last longer, and costs will come down more that way.

Dani Eder/Boeing/Advanced Space Transportation

Re: EEC Product Liability

John Gilmore <hoptoad.UUCP!gnu@cgl.ucsf.edu>
Sun, 13 Dec 87 05:13:40 PST

> For imported goods, the original importer into the EEC is liable.

I am curious how long the US->European email/netnews gateway at mcvax will last after its first suit under this Directive. Plenty of buggy PD and redistributable software enters the EEC this way; in fact, it may be the largest single channel for import of software.

> It is expected that the Act will greatly increase the adoption of software
> Quality Assurance (to conform to ISO standard ISO 9001) and the use of
> mathematically rigorous specification and development methods (VDM, Z etc).

Note that this is posted by someone who makes his living selling such products (at Praxis). I would say "caveat emptor" but clearly in Europe this no longer applies.

It might be fun for someone to sue Praxis for bugs in their product, especially bugs that result in delivered systems with undiagnosed failures which later cause suits.

Does Lloyd's of London sell "bug insurance"?

The Presidential "Football"...

<hplabs!motsj1!motbos!mcdham!carl@ucbvax.Berkeley.EDU>
Sat, 12 Dec 87 10:17:19 PST

I am looking for information related to the "Black Box" that is supposedly near the President at all times. This box is reportedly the control center from which the President can authorize a nuclear launch. I have heard it referred to as "The Football".

Can anyone tell me anything about it? Even folklore is acceptable. Are there any texts with this information in it?

Whatever you could let me know would be a help. I am writing a fictional

account of a Nuclear War and need the inforrmation to complete the work.
Thanks in advance for your help.
Carl Schlachte

[Folklore may be OK for Carl, but please provide him with
folklore privately, and keep RISKS messages factual. PGN]

Radar's Growing Vulnerability

Jon Eric Strayer <ndq@h.cc.purdue.edu>
Thu, 10 Dec 87 15:51:10 EST

>From: Peter G. Neumann <NEUMANN@csl.sri.com>
... (RISKS readers will recall that the British investigation concluded that
the Sheffield's own radars were jammed by a communication back to London that
was being held at the time.)

While there are anti-radiation missiles, the Exocet that hit the Sheffield was not one of them. I also have serious doubts that the Sheffield's radars were "jammed" by a communication transmitter. I understand that the radars (and ESM/ECM equipment) were shut off because they jammed the comm equipment.

[Yes, that was one report. Sorry I turned it around. PGN]


Search RISKS using swish-e

Search RISKS using swish-e

THE RISKS DIGEST

Forum on Risks to the Public in Computers and Related Systems

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

Volume 5: Issue 74

Monday, 14 December 1987

Contents

Rounding error costs DHSS 100 million pounds

Robert Stroud <robert%cheviot.newcastle.ac.uk@NSS.Cs.Ucl.AC.UK>
Mon, 14 Dec 87 09:45:00 GMT

This is an extract from a front-page report in the Independent (12 Dec 1987). It would appear that for over a year, due to a programming error, the government have been underestimating inflation by 0.1%. The cumulative effect of this error on index-linked payments such as pensions amounts to 100 million pounds which they have a statutory obligation to pay back.

The interesting question this poses is what level of error would be considered reasonable in calculating inflation. Even a 0.001% error would cost 1 million pounds by this reckoning, and yet averaging the price of commodities introduces

spurious accuracy when in practice prices will be to the nearest 0.5p.

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

"DHSS in 100m pounds inflation blunder - pensioners to get payment after computer error" by Steve Levinson and Colin Hughes

Reproduced without permission from The Independent (Sat 12th Dec 1987)
Copyright (c) Newspaper Publishing PLC 1987

More than nine million pensioners are shortly to receive a tax-free lump sum bonus of between 7.50 and 12.00 pounds after the Government yesterday admitted that a computer error had led to publication of incorrect inflation figures for the past 21 months.

The pay out to pensioners will cost an estimated 100 million pounds, but other social security recipients, who include some of the poorest, will not be reimbursed for the error which has meant that benefit increases have not kept pace with inflation.

[... Lots of stuff about how the government will only reimburse those benefits for which it has a legal obligation or has made a pledge to keep pace with inflation, despite the fact that most other forms of benefit are usually raised in line with inflation, and how this is likely to cause a political row(!) ...]

Although the computer error at the Department of Employment has meant an understatement of only 0.1% in inflation, it is difficult to conceive of a more embarrassing mistake or one that affects more people. Pay negotiators, taxpayers, savers, and pensioners are all caught up in its implications.

The department does not intend recalculating past inflation figures, but says that yesterday's 4.1% rate for the year to November is correct. The error itself is put down to a mistake made early last year when a programmer, seeking to speed up the process of analysing each month's prices, entered details for household goods which omitted everything after the decimal point. [I assume this means pence rather than pounds!]

Nobody noticed and from January this year the new program was given wider application to other goods, including clothing. The effect was that all Retail Price Index numbers [the official measure of inflation] between February 1986 and January 1987 were 0.06 points too low, and after January 1987, a further 0.09 understatement was added. The error was spotted purely by chance only last month when a new attempt was made to speed up the process of analysing price information.

Computers' Role in Stock Market Crash

Rodney Hoffman <Hoffman.es@Xerox.COM>
13 Dec 87 22:05:59 PST (Sunday)

The Friday, Dec. 11 'Wall Street Journal' ran a story headlined "Were Computers a Help or a Hindrance? Securities Industry Asks After the Crash" by Michael W. Miller. It was one of several articles trying to put the recent crash in perspective. What's particularly interesting is that the piece is not narrowly focused on the role of computers in the crash. Instead, it's a thoughtful questioning of "the ways computers changed Wall Street". The whole article is well worth reading. A few edited excerpts:

> Portfolio insurance, index arbitrage and other modern Wall Street trading innovations that depend on ever speedier and more complex trades ... wouldn't have been possible with the more than 200 Tandem TNX and TXP computers of Securities Industry Automation Corp. (SIAC), run by the New York and American stock exchanges.... SIAC's system is one of the biggest collections of computer power gathered under a single roof. Its workings have grown so vast that today SIAC uses computers to keep track of all its computers.
>
> Did electronic analysis and trading produce a whole new breed of high-tech investors whose criteria have nothing to do with the traditional corporate and economic forces behind stock movements? "I think there is a tendency today to substitute trading for investment," says former U.S. Attorney General Nicholas deB. Katzenbach, who was commissioned last spring to study program trading for the Big Board. "Computers are an element of that, sure. but I don't think it's just because of computers." Which came first?...
>
> One way or another, the computer has transformed the stock market in ways unimaginable even a few years ago. ... The volatile growth is "a real monster, and it's obviously one that we cannot control," a top SIAC official says. In many ways, Wall Street was an unusually ripe target for computerization. Nowhere does faster, better information command such a high premium....
>
> In hindsight, it seems that computers on Wall Street created an appetite they ultimately couldn't satisfy. Following the classic addicts' pattern, each time investors got more powerful computers, they developed investment techniques that needed even more powerful computers....
>
> A rethinking of computer-aided trading in inevitable... But curtailing powerful technology already in wide use isn't easy -- as any arms negotiator can attest.... Moreover, Wall Street is worried about what the Japanese may come up with. A state-of-the-art futures market is scheduled to open in Tokyo in March. Observes Ramon Villareal or Tandem: "Once you've got the tools, if you don't use them, someone else will."

The Infarmation Age

Ivan M. Milman <ivan@sally.utexas.edu>
Mon, 14 Dec 87 23:00:50 CST

The business section of the December 14th (Monday) edition of the Austin American-Statesman had a 4-column feature article entitled "Modern farmers plow profit with computers." The article discussed at great length all the benefits farmers are receiving by using computers.

Directly below the article is a section called "In Brief", and the first headline is "Computer Trouble." The paragraph described how the report of humidity and soil temperatures provided every week by Blackland Research Center was interrupted due to computer troubles.

Ivan Milman

[Perhaps the computer was affected by humidity? PGN]

Virus programs and Chain letters

David G. Grubbs <dandelion.CI!dgg@husc6.harvard.edu>
Sun, 13 Dec 87 20:50:57 est

When do we start treating these foolish, destructive, puerile acts as they deserve?

Virus programs and Chain letters are not harmless pranks, as most of the comments I've read lately seem to imply. They waste immense amounts of our two most precious resources: time and effort. And they are, to my mind, evidence of an anti-social behavior which deserves to be actively suppressed, even attacked.

Persons caught sending a chain letter should have their mail privileges suspended for some period, as a first offense, then removed entirely if the idiocy continues.

Persons writing or distributing Virus programs should be warned, then kicked out of whatever organization is affected, from a place of employment to whatever social group is involved. A prank without an appreciative and approving audience is an anomaly. Remove the audience and the act becomes meaningless.

It is not possible to legislate maturity, termperance or responsibility, but it IS possible to influence one's peers through social pressure. These acts are intolerable and it is up to YOU to do something about it. Stop chuckling at juvenile acts of destruction. Let the perpetrators know they are out of line, take steps to stop them and share the ideas that work with the rest of us.

"If you aren't part of the solution, you will become part of the precipitate."

David G. Grubbs, Cognition Inc., 900 Tech Park Drive, Billerica, MA 01821
UUCP: ...!{mit-eddie,talcott,necntc}!dandelion!dgg (617) 667-4800

Baby monitors can also be very efficient "jammers", too.

Rob Warnock
7 Dec 87 20:25:16 GMT

I was recently involved in helping with the logistics and security for a large (several K people) outdoor event in Vermont, and we decided to use a bunch of those Radio Shack "bug ears" short-range FM transceivers for communications among monitors who would be spaced throughout the crowd to handle medical emergencies, lost children, etc. Well, everything worked just fine, until some VIPs started showing up a day or two ahead of the main event. Suddenly, the 49 MHz band that the transceivers use began to be jammed with a strong carrier, with a lot of 60 Hz "hum" and no (apparent) modulation. The "jamming" came and went at various times, for several hours at a time. We began to be worried that our careful public safety plan was going to be destroyed by this "jamming"!

Finally, during a period of "jamming", we heard a loud baby cry, followed by a door opening and the soothing tones of a mother. Problem solved! (...after some diplomacy, that is.) We were able to recover our public safety plan by convincing the parents (who were fortunately part of the sponsering group) to leave the baby monitor "off" during our practice drills, and during the entire day of the main event.

What's the "Risk"? Both the short-range transceivers and the baby monitor use the 49 MHz "public domain" band, which is the same band used by many cordless telephones. (We had in fact thought that the "jamming" was a cordless phone.) Who is to adjudicate conflicts when they arise? The FCC regulations specifically state that any such device "(1) May not cause any harmful interference to any other service; and (2) Must accept whatever interference [that arises] from any other [licensed] service."

As more and more "deregulation" occurs and more and more "consumer" R.F. (and infrared) devices show up on the market, conflicts of this type will increase. I only know that not all of them will be settled so amicably as the one described above.

Rob Warnock, Systems Architecture Consultant

UUCP: {amdcad,fortune,sun,attmail}!redwood!rpw3
ATTmail: !rpw3
DDD: (415)572-2607
USPS: 627 26th Ave, San Mateo, CA 94403

The Saga of the Lost ATM Card

Alan Wexelblat <wex%SW.MCC.COM@MCC.COM>
Mon, 14 Dec 87 10:06:09 CST

Last week, I went to my bank to order a new ATM card. Here's why:

First, some background. Austin is served by two major ATM networks, Pulse and MBank. Each accepts the others' cards for purposes of withdrawals and transfers, but not deposits. Very convenient - Pulse is a national network and

friends from Philly have been able to get cash while in town.

Saturday night I was in a supermarket buying food to bring to a friends' dinner. I realized I didn't have enough cash, so I used the ATM. It was MBank, but it had a big sticker indicating it would accept my Pulse card, so I tried. I got the cash and the receipt, but the machine didn't return my card. I went to the supermarket service desk.

They helpfully informed me that they had no way of retreiving my card, but if I was willing to hang around for a while "...the machine will probably spit it out." Does this happen often, I asked. "All the time. Usually the card comes back in less than 10 minutes. Sometimes it comes back when the next person tries to do a transaction."

Well, I'm late for dinner, so I can't wait around. Fortunately, I'm with a friend and he has bank cards. First, he tries one for an account he knows is defunct. The machine rejects it. Then he tries his MBank card (brave fellow - how does he know his card won't get swallowed, too?). Both are returned by the machine, but my card stays gone.

After a useless call to the MBank service number (answered by a security guard who knows nothing) we leave. I'm told that they empty the machines first thing Monday morning, and I should get a phone call then.

When Wednesday rolls around and I haven't heard, I put in a call to MBank's service number. I explain my situation to a service rep who, upon finding that I'm not an MBank customer clams up. I have to call *my* bank, she says, and get the card back from them. Can she check and see if my bank has the card? No. Does she care that her bank's machine is regularly eating cards and spitting them back at random intervals? No.

So I call my bank's central customer service number and I'm told that they still don't have the card. But even if I did, I'd have to get a new one. MBank returns them cut up, you see. Why? Because they consider it too risky to mail the cards intact to my bank. My bank has no trouble mailing the cards to me. But I'm a reasonable person, perhaps I can go to MBank and identify myself and get my card back directly from them? No... "Customer identification is the problem of the owning bank." Not that I can explain to this imbecile that it doesn't matter whether my bank can identify me, since all they could give me would be useless plastic scraps...

So now I have to wait 4-6 weeks for the central office to produce another card. Fortunately, the PIN is not on the card, so my wife's card is still usable. Anyone want to guess at the number of MBank machines I'll be using in the future?

--Alan Wexelblat

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

Interchange of ATM Cards

<TMPLee@DOCKMASTER.ARPA>

Mon, 14 Dec 87 00:32 EST

Although the details, especially the time period, are now fuzzy (perhaps someone else from Minnesota can fill them in), it seems appropriate to note that sometime after ATM's and competing ATM networks started to become popular the Minnesota legislature passed a law REQUIRING that ALL ATM's accept each other's cards. The law was virtually unheralded. I seem to recall being quite surprised when, either by accident or out of idle curiosity, I first discovered that the card for one network would work on another. Most of the machines now carry notices listing all of the other cards they will take; originally there was no such notice.

PacBell Calling Card Security (or lack thereof)

Brent Chapman <chapman%mica.Berkeley.EDU@violet.berkeley.edu>
Sun, 13 Dec 87 21:36:14 PST

I just recently got my new Pacific Bell Calling Card. On the sheet describing where, how, and why to use your card, there is a section (quoted):

> It's Secure. Your Calling Card Number is made up of your billing number and a four-digit Security Code. Your Calling Card cannot be used without this Security Code, so you are protected from unauthorized calling as long as you keep your code safe.

Sounds good, right? Standard stuff. _BUT_, elsewhere ON THE VERY SAME PAGE, in the descriptions of where you can use your card, you find (emphasis mine):

> At Pacific Bell Credit Card Phones: You'll find new Pacific Bell Credit Card Phones at airports and hotels near other Pacific Bell coin and coinless phones. These, which will be appearing at many other locations as well, allow you to simply insert your Calling Card and press the number you want. YOU DON'T EVEN NEED TO GIVE YOUR SECURITY CODE, BECAUSE THE MACHINE READS IT FROM THE CARD.

Gee, ain't technology wonderful? Any bets that only PacBell can read the code from the card?

Brent Chapman Capital Market Technology, Inc.
Senior Programmer/Analyst 1995 University Ave., Suite 390
{lll-tis,ucbvax!cogsci}!capmkt!brent Berkeley, CA 94704
capmkt!brent@{lll-tis.arpa,cogsci.berkeley.edu} Phone: 415/540-6400

> [If your card is lost or stolen, who needs to read the security code? By the way, there were several other messages along these lines, including one from David Robinson. PGN]

IBM invaded by a Christmas virus

Franklin Davis <fad@Think.COM>
Mon, 14 Dec 87 09:38:55 est

> This article seems to have a lot of things in it that the reporter didn't understand. I assume that the "terminals" in question are really PC's connected to the mainframes; for one thing.

Probably the users were connected by 3270 type terminals (or emulations on a PC) which use a half-duplex block mode protocol. If you turn off such a terminal your session is aborted, and you lose current edits. It is also very difficult to interrupt an executing program, since it "owns" the line. There is a "system-attention" key, but a busy system may take literally minutes to respond. (I'm glad I don't have to use an IBM mainframe any more!! :-)

--Franklin Davis Thinking Machines Corp. fad@think.com

Search RISKS using swish-e

THE RISKS DIGEST

Forum on Risks to the Public in Computers and Related Systems

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

Volume 5: Issue 75

Tuesday, 15 December 1987

Contents

Advice to the Risklorn

Steven McBride <shamus@BOEING.COM>
Tue, 15 Dec 87 10:40:20 pst

Franklynn Peterson and Judi K-Turkel in their newspaper column "The Business Computer" {(c) 1987 P. K. Associates, Inc.} discuss computer problems with banks, phone companies, and supermarkets. The discussion on phone billing which follows was new to me -

> Ripped off by computer mistake? Fight back
>
> . . .
>
> Before computerization, your phone company didn't charge you if nobody picked up at the other end. Now, if there's a busy signal or no answer to your ring, you may get charged for a one-minute call. Unless you keep track of all your calls you may never even notice it.
>
> Has your bill ever shown two different minute-long phone calls made during the same minute of the same day? Ours has. It's a dead giveaway. It proves our servicer's computer can't tell a non-answer from a completed call.

Many states have watchdog public service commissions. Ours specifies that we can't be charged for calls that reach nobody. But it also lets the phone company bill us incorrectly. The burden's on us to go through each bill circle all disputed charges, and write letters explaining why we're not paying them.

These charges can mount up fast if you're phoning via computer. . .

. . .

Here's what's sad about all these computer-made annoyances: They're unnecessary. These very computers are capable of doing consumer-pleasing tasks at a penny a job. Why don't they? Because whoever bought them, programmed them, and manages them obviously doesn't want a system that can help customers. They want what's fastest or cheapest to design, easiest to manage, and most profitable for the firm.

How can we change things? By joining in making the status quo grimmer than the task or reprogramming to give better service.

We changed supermarkets when our once-favorite store refused to give pre-checkout pricing clues.

We deduct from our phone bills all one-minute calls, putting the burden on the long distance carrier to show it any were completed.

And when we clear up a blunder our bank's computer makes, we bill them a service charge. You're welcome to join us!

<minow%thundr.DEC@decwrl.dec.com>

(Martin Minow THUNDR::MINOW ML3-5/U26 223-9922)
Date: 15 Dec 87 08:06
To: risks@csl.sri.com
Subject: Interesting note on expert systems liability from AI-Digest

From: DECWRL::"AIList-REQUEST@SRI.COM"
"AIList Moderator Kenneth Laws 14-Dec-87 2224 PST"
AIList Digest Tuesday, 15 Dec 1987 Volume 5 : Issue 283
...
Date: Thu 10 Dec 87 10:27:39-PST
From: George S. Cole <GCOLE@Sushi.Stanford.EDU>
Subject: Expert System Liability

I have researched this area and a paper is forthcoming -- as soon as the USC Computer/Law Journal editorial staff are ready -- on "Tort Liability for Artificial Intelligence and Expert Systems". The trite answer is yes, there can be a suit and EVERYBODY INVOLVED will be named -- because the plaintiff's lawyer will realize that the law does not clearly know who is liable (including the plaintiff).

A short answer is to cite the Restatement of Torts, 2nd, Section 552: "Information Negligently Supplied for the Guidance of Others:

one who, in the course of his business, profession, or employment, or in any other transaction in which he has a pecuniary interest, supplies false information for the guidance of others in their business transactions, is subject to liability for pecuniary loss caused to them by their justifiable reliance upon the information, if he fails to exercise reasonable care or competence in obtaining or communicating the information".

This section was cited without success in Black, Jackson and Simmons Insurance Brokerage, Inc. v. IBM, 440 N.E. 2d 282, 109 Ill. App. 132 (1982). The phrase "in the course of his business" was strictly construed to prevent liability under this cause of action (there were others, including warranty) as the court noted that the defendant had sold both hardware and software to allow the firm to process information. But in Independant School District No. 454, Fairmont, Minnesota v. Statistical Tabulating Corporation, 359 F. Supp. 1095 (N.D. Ill, 1973) the court permitted a negligence action to be brought against the third-party statistical bureau whose miscalculations had led to the under-insurance of a school which had then burned down. The court stated: "[O]ne may be liable to another for providing inaccurate information which was relied upon and caused economic loss, although there was no direct contractual relationship between the parties...The duty to do work reasonably and in a workmanlike manner has always been imposed by law..." Factors the court suggested to consider included (1) the existence, if any, of a guarantee of correctness; (2) the defendant's knowledge that the plaintiff would rely upon the information; (3) the restriction of potential liability to a small group; (4) the absence of proof of any correction once found being delivered to the plaintiff; (5) the undesirability of requiring an innocent party to carry the burden of another's professional mistakes; and (6) the promotion of cautionary techniques among the potential defendants for the protection of all potential plaintiffs.

Did the ES indeed make a mistake? Suppose Joe has said he plans to invest for 15 years -- too short for real estate, too long for bonds, and in that light the "Black Monday" might be seen as a temporary aberration. (I.e. Joe caused the harm by selling out at the bottom rather than holding on for the 15 years as planned.)

Can the experts hide behind the company? Those who are professionals (which is a legal phrase for "holders of a semi-monopoly") probably cannot be fully shielded; the rest may have to seek indemnity from their corporation. It will depend in part on their employment contract, or lack thereof.

Can the knowledge engineers be found liable if their mistake led to this? What sort of mistake? A standard programming flaw is not the same as a design flaw. What if the mistake lies at the boundary -- who is responsible for realizing that the computer has to have rules for assessing "market psychology" that will quantitatively assess the subtle dynamics of what the current "feel" for the market is? Did the domain experts learn that the computer was going to do more than crunch numbers?

This is both a nascent and a complex legal area. My hope is that a number of the AI and ES companies realize the potential exposure and that the evolution of the law can be influenced by their behavior -- and begin to plan defensively. It is a bit more expensive initially, affecting immediate profits; but it can provide tremendous savings both for the firm and for the industry over the longer run.

George S. Cole, Esq.
793 Nash Av.
Menlo Park, CA 94025
GCole@Sushi.stanford.edu (until it goes away)

Re: Can you sue an expert system (RISKS DIGEST 5.71)

George Bray <lcc.ghb@SEAS.UCLA.EDU>
Tue, 8 Dec 87 16:28:09 PST

The discussion of suing expert systems is similar to the issues raised by [the case of the Therac 25]. I am talking about the several deaths and serious injuries that have resulted from software failures in certain X-Ray machines made by Atomic Energy Canada. (See the latest issue of IEEE Spectrum for a short summary article; an earlier issue (within the last year) of IEEE Spectrum had a longer article on the same topic.)

Basically, a modification to the data entry software used by operators resulted in the machine delivering extremely large doses of radiation while indicating that only small amounts were delivered. As I remember it, the machine can generate electron beams directly, or use the electron beams to generate X-rays. The machine is supposed to lower a target into the path of the beam to generate the X-rays.

Apparently, when the operator did some kind of data editing operation (I think it was use an up-arrow key), the software would get confused and raise the target while setting the beam intensity to the huge values needed to generate X-rays. This editing code was added in response to user's complaints about the primitive data entry in earlier versions of the software. If I remember correctly, the failure was caused by some rare conjuction of situations that could occur if the operator used the "up-arrow" key to edit data at just the right time. I think the bug was some variable that was also used in an interrupt routine.

Various family members of those injured or killed have sued everyone responsible, including the software engineer who added the "user-friendly" editing code. This raises many issues. On the one hand, there was no doubt that the software bug killed and injured people, so it seems reasonable that the people who made the poor software are liable. On the other hand, I believe that the bug was due to an unforeseen interaction that would be very hard to eliminate. These kinds of bugs probably exist in much of the software in thw world.

What do RISKS readers think of the issues raised by this case? Are programmers liable for their software's actions?

George Bray, Locus Computing Corporation

Litigation over an expert system

Dean Sutherland <Sutherland@TL-20B.ARPA>
Tue, 8 Dec 1987 09:43 EST

In Risks digest 5.71, chapman@russell.stanford.edu (Gary Chapman) mentions a "goofy" California law that provides for a defendant who is only 1% responsible to pay 1% of the judgement. Although this law may be goofy, it is a major improvement over previous versions. Before this law was passed, it was possible to have the following situation:

Defendant A: 99% guilty, has assets of $10,000
Defendant B: 1% guilty, has assets of $1,000,000,000
Judgement of $10 million against defendants. A pays $10,000 (or maybe nothing by declaring bankruptcy). B pays $9,990,000... EVEN THOUGH B WAS FOUND TO BE ONLY 1% GUILTY.

The new version of the law is a BIG improvement.

Dean F. Sutherland, Tartan Labs

Expert Systems Liability

Bjorn Freeman-Benson <bnfb@june.cs.washington.edu>
Tue, 08 Dec 87 12:09:03 PST

Regarding the discussion of Expert System Liability in RISKS-5.69 through 5.71 --- one argument is "it's just like a book". I disagree. The fact is that a book is completely Passive, but an expert system may be Active. One must ask a book for advice, but the expert system may offer advice on its own, or even act in your behalf.

Consider a car with expert system controlled drive-by-wire steering. When it fails, the manufacturer is liable, and it may turn out that the expert system made an erroneous decision. In that case, who, in addition to the automobile company, is liable?

Bjorn N. Freeman-Benson,University of Washington

Sue Who? (Re: RISKS-5.71)

William Swan <uw-beaver!tikal!sigma!bill@RUTGERS.EDU>
Tue, 8 Dec 87 11:07:24 pst

>From: "Jerry Leichter (LEICHTER-JERRY@CS.YALE.EDU)"
>Subject: re: Can you sue an expert system
>[...] "If an expert system gives bad advice, who can I sue?" I find it
>extremely disturbing that this is considered an interesting question by
>ANYONE, let alone by technically sophisticated people. It is a symptom of
>the pervasiveness of our misplaced trust in buzzwords and, more generally,
>in computers: If the computer said it, it MUST be right. [...]

I wonder.

You believe instruction manuals, don't you? And try to follow the procedures therein? I can show you a service manual for my pickup that is very wrong at one step.

A true story:

Last week I was dealing with a new copier, which had its "entire" manual on-line. I needed to do two-sided copies and was overwhelmed by the numerous

buttons and cryptic icons on the thing. No problem, I pressed "help" and the display walked me through the setup. Very nice! It even walked me through clearing a paper jam or two - even telling me where within the machine the paper jammed and how to get there ("lift lever A", "raise lid B", etc).

Suddenly I got a message, "remove paper from duplexor". What's a duplexor? I pressed help, and got.. "remove paper from duplexor". I checked all the mechanics on top. No paper. I cleared the paper trays. Nothing out of place. I opened the doors to the insides, the display says "close front door". I close the door and look elsewhere. Nothing. I open the doors again, it says "close front door". I close the doors and cycle power on the machine. I try a copy, it says "remove paper from duplexor". I open the machine up (it says "close front door") and hunt through the innards. No paper.

Finally, I find a secretary (it's after hours but she's still there) who tells me what a duplexor is and where it is. I return to the machine, open the doors (it says "close front door"), find the duplexor and remove the sheet, close the doors (it says "ready") and continue copying!

What did I do wrong? Believe the computer? I don't think so (C'mon, I know better than *that* :-). I had instead been led to put my trust in an incomplete set of procedures. More knowledge (i.e. what a "duplexor" was) would have helped prevent me from making this error.

The problem I ran into, and one that I'm sure we'll see more and more often, is that this form of the information hid its incompleteness. If I had had a printed manual with no reference to "duplexor" I would have known it was incomplete. This mechanised manual hid that information from me and, worse, led me astray by behaving as if it were not incomplete.

If this had been a situation with serious consequences I believe I would have very good cause for litigation.

---

re: Can you sue an expert system (RISKS-5.71)

Wm Brown III <Brown@GODZILLA.SCH.Symbolics.COM>
Wed, 9 Dec 87 17:55 PST

From: "Jerry Leichter (LEICHTER-JERRY@CS.YALE.EDU)"
<LEICHTER@VENUS.YCC.YALE.EDU>
Subject: re: Can you sue an expert system

In RISKS-5.69, Barry Stevens becomes another in a long line of people to raise the question "If an expert system gives bad advice, who can I sue?" I find it extremely disturbing that this is considered an interesting question by ANYONE, let alone by technically sophisticated people. It is a symptom of the pervasiveness of our misplaced trust in buzzwords and, more generally, in computers: If the computer said it, it MUST be right.

I find it extremely disturbing that ANYONE on this list would make such a statement. Judging from the length of the diatribe which followed this preamble, I must conclude that Mr. Leichter really has strong feelings and

quite a lot to say on the subject, and therefore must find it somewhat more interesting than he admits to. Personally, I think that the realities of turning software, especially expert systems, loose on the world are very close indeed to the center of this forum's domain.

When software of this type is sold to professionals who know its limitations, or who understand that its output is an 'opinion' rather than a statement of hard facts, I agree that it is not reasonable for those users to turn around and sue if they get burned by depending upon it. This, however, is a very small subset of the potential users for expert systems.

Lawsuits are society's way of enforcing product specifications and warranties. Taking away this mechanism is equivalent to voiding these contracts. One way to look at things is that this is an important check which will discourage the offering of immature or inferior products. It is a very effective way of making marketeers "Put their money where their mouth is."

There are definitely cases where expert systems are of value because they offer potential savings in time; consider an 'advisor' for hospital emergency rooms which gives every third-shift physician the knowledge equivalent of twenty top specialists and a medical library, but much quicker. Users of this system simply won't have the time to second guess the 'expert' or cross check every literature reference, but if this system gives incomplete advice it will sooner or later kill someone. Should the physician on duty be responsible for deciding whether to follow the system's advice, even if he doesn't understand the specialty involved? Should the hospital let some patients die for lack of quick decisions rather than buy this system? Should state legislatures indemnify some or all of the players from lawsuits, thus legitimizing the concept that anything the computer says is gospel? Clearly, the legal aspects will be a large factor in the equation which decides when or if such systems will be installed.

On a more mundane scale, consider the original example of a personal finance advisor. If it is offered as a novelty, with pages of disclaimers and explainations of why no sane person would rely on its advice, who will buy it except as a toy? On the other hand, if it comes with the usual marketing banners describing it as the answer to everyone's financial questions, the end user certainly has some right to expect that it will give good advice. Whether this right extends to the point of filing lawsuits is properly a matter to be decided by a jury, based upon the facts in each individual case; it would be just as wrong to give blanket protection to software vendors as it would be to legislate all responsibility onto their shoulders.

To say that this topic is complex or ill-defined is an understatement. To say that it is not interesting is a personal opinion which I will hotly contest. If expert systems are to progress from academic curiosities to everyday-life applications, they will have to be useable by non-computer types who need fast and reliable answers, not philosophical disertations or legal disclaimers.

NOTE: The opinions expressed are my own and do not necessarily represent those of my employer or anyone else.

Microprocessors vs relay logic (RISKS-5.65)

Wm Brown III <Brown@GODZILLA.SCH.Symbolics.COM>
Wed, 9 Dec 87 17:55 PST

Two cents worth on the relative virtues of microprocessors vs. relay logic for railway control systems. (Continuing the discussion started in RISKS 5.65).

There is such a thing as choosing the right tool for a job. About fifteen years ago, I did some design work on a motion control system for amusement rides. The improvements since then in reliability and cost of mini and micro computers has changed things, and I don't know whether I would draw the same conclusions today, but at the time the best solution appeared to be relays with a mini backing them up and monitoring for control system failures. Here's why:

<>>Well designed relays have a conservative life expectancy of 100 million operations (that's 1E8). They don't particularly care how long each operation lasts; things only wear when they move. Given a typical rate of 100 operations per hour, this works out to 1 million (1E6) hours of ACTUAL USE before they start to die. Idle hours don't count.

Computers typically have a fairly constant MTBF, regardless of what they are doing for those hours. Turning them on and off may substantially reduce this time, so it is difficult to decide whether it is better to leave the system on all day and use up 24 hours of life per day or power it on and off every day. Either way, not many computers come close to the million-hour level.

<>>Somewhere in the system, your controller has to connect to a real world full of spikes, transients, dirt, water, and unionized maintainence techs with 250 watt soldering irons. Relays are pretty imune to nearby lightning hits, poylester shirts, etc. Anything which permanently damages them tends to make them fail completely.

Computers can be brought down by anything from dry days to alpha particles. Worse yet, they may drop a bit without noticing it and you will never be able to figure out exactly what happened. Yes, it is feasible to program in a lot of redundancy, but it is still possible for a glitch in the housekeeping routines to clobber the functional code or working storage.

<>>Flexibilty is great when you want to control a ride and balance your checkbook on the same machine, however there are some cases where the same flexibility is useless or even dangerous. If you want the system to perform the same way, day after day, it is tough to beat hardwired control logic. If something DOES go wrong, it is usually much easier to deduce how and why when the logic paths are soldered down.

<>>Failures in relay logic tend to be more localized. A stuck contact in track zone 5 may someday permit one car to tail-end the next, but it won't affect zone 8 at all. If the same CPU is controlling the entire system it can spread havoc everywhere instantly.

No, I don't sell relays or even use them any more. This just seemed germane to the original discussion.

Search RISKS using swish-e

THE RISKS DIGEST

Forum on Risks to the Public in Computers and Related Systems

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

Volume 5: Issue 76

Wednesday 16 December 1987

Contents

Designing for Failure

Don Wegeng <Wegeng.Henr@Xerox.COM>
16 Dec 87 15:59:38 EST (Wednesday)

In RISKS 5.75 Wm Brown III makes some interesting observations about the reliability differences between microprocessors and relay logic (prompted by a discussion about using microprocessors to control railroad switching). What I would like to discuss here is how systems react when a portion of the system *does* fail. Since I am involved in the design of microprocessor-based

real-time control systems, this area is of great interest to me.

In my opinion designers should always consider the worst situation that can result from the failure of a component. Part of this should include determining what events might be missed or ignored if a particular component fails. The system's reaction to the component failure must take these events into account. For example, a microprocessor might be used in a robot arm to monitor an electric eye that detects when something is in the path of the arm. If the microprocessor fails the system's reaction must include whatever it would do if the electric eye beam had been broken, for there is no way for the system to determine the state of the beam (and it must assume worse case). Note that all of this does little good if the system does not detect that the microprocessor failed (and detecting the failure may be a bigger problem than reacting to it).

Computer control has the potential to allow greater flexibility than previous technologies. This flexibility brings with it new risks (which have been discussed many times in RISKS). It is essential that such systems be designed so that their reaction to failures will be predictable and safe.

Don

Computer MTBF and usage

Andy Freeman <ANDY@Sushi.Stanford.EDU>
Tue 15 Dec 87 19:20:17-PST

Wm Brown III <Brown@GODZILLA.SCH.Symbolics.COM> writes:

> Computers typically have a fairly constant MTBF, regardless of what they are doing for those hours. Turning them on and off may substantially reduce this time, ...

Professor Ed McCluskey at Stanford has shown that the MTBF of computer systems does depend on usage/load. This isn't surprising for software, but I remember seeing something (in an abstract) about how load affects hardware failures as well. It was surprising enough to remember, but not interesting enough for me to investigate further.

-andy

Liability and software bugs

Nancy Leveson <nancy%murphy.uci.edu@ROME.UCI.EDU>
Tue, 15 Dec 87 19:20:03 -0800

In Risks 5.75, George Bray writes with respect to the Therac accident:

> >On the other hand, I believe that the bug was due to an unforeseen
> >interaction that would be very hard to eliminate. These kinds of bugs
> >probably exist in much of the software in thw [sic] world.

If a reasonable person would agree that bugs exist in much of the present software, then it seems that it is also reasonable that features be built into the system to protect against such bugs. Non-computerized versions of such

machines usually contain interlocks to prevent such catastrophic behavior. These same interlocks can be built into the software (or into the hardware) to protect against software errors. If it is standard practice to include such features by hardware engineers, should it not be standard practice for software engineers? Shouldn't somebody have thought to include "reasonableness" checks in the AECL software? I have heard aeronautical engineers speak of a "safety envelope" and seen them include design features to detect when the safety envelope is violated and to recover from such events. It is often possible to determine the "safety envelope" of software behavior and include checks when it is being violated. Of course, checking routines can also have bugs in them, but they are often much simpler than the original software and provide an independent check that reduces the risk, probably significantly.

Do we teach programmers to expect software errors and to build the software to detect and handle erroneous or unsafe states resulting from software bugs? If manufacturers of hardware devices can be sued for not taking reasonable care by including safety features in their devices, couldn't manufacturers of software be similarly liable for not doing the same?

[By the way, for those interested, I have heard that AECL has settled out of court with the families of the victims. There is still one suit outstanding in which the hospital where two people were killed is suing for their money back. They do not believe that the problems have truly been fixed and do not want to use the machine anymore. One might note that AECL claimed the problem was fixed before a third person was killed a year ago in Yakima].

Nancy Leveson, UCI

Re: Need for Reporting Systems

<pgarnet@nswc-wo.ARPA>
Wed, 9 Dec 87 14:09:01 est

In Risks 5.71 Eugene Miya suggests

< If we are ever going to progress out of the software muck, we are going
< to have to come up with mechanisms to replace all of our anecdotal
< information with better information.

I agree. One part of the 'software muck' is illicit code, e.g., Trojan horses, viruses, etc. It is EXTREMELY difficult to obtain any examples of illicit code, as any organization which has been bitten by one of these bugs does not want to be responsible for exacerbating the situation by letting the illicit code out to possibly infect another system.

The software security community needs to study the diseases which we are trying to defend against, as potential defenses created in a vacuum of information will only work in a vacuum. A clearinghouse, repository, library, or whatever name one wants to give to such a function should be set up so that those of us who are trying to build defenses can have subjects to study.

There are, however, a number of sticky issues revolving about setting up such a clearinghouse.

1) How do you trust the repository? How does one know that information given to the repository will not be abused, nor will it be used against the giver?

2) How does the clearinghouse know who to disseminate which information to in order not to violate issue number 1? How does one decide on who has a legitimate need to see 'dangerous' information, e.g., details on viruses, trap doors, etc.

3) The clearinghouse must not be an information sink, sucking up information from anyone willing to donate their examples but never giving any information out. It must be clear that the purpose of the clearinghouse is to facilitate the sharing of information in a non-threatening way.

4) The clearinghouse must not be an organization that people are inherently scared of, "If I tell them what happened, what are they going to do to me?"

5) There must be some mechanism to validate the information coming to the clearinghouse to insure that it is correct. We do not want a repository of misleading, invalid data.

6) Who's going to pay for this service?

There are organizations which collect information about computer crime. One which immediately comes to mind is SRI. Maybe this or some other organization could be a starting point?

One issue which will certainly come up in trying to collect, organize, and disseminate this information will be classification. Is the data unclassified, classified (C,S,TS,...), sensitive, proprietary, ...? I believe that if issue number one, trust in the clearinghouse, is solved, the issue of putting information in its proper category is administratively solvable.

I could see great value in collecting examples of illicit code (and, of course, corresponding risks). What have people really done? How can we learn from the examples? What generic technical defenses can be developed which specific companies/organizations can then apply to their systems?

Anyone interested in discussing these issues in a workshop setting, either classified or unclassified, commercial or government - please contact me.

Maybe we can come up with a workable mechanism to not only replace all of our anecdotal information, but to persuade some of the hidden information to come out of the woodwork.

Paul Garnett (pgarnet@NSWC-WO.ARPA)

Tom Swift and his Electric Jockstrap

<"Arthur_Axelrod.WBST128"@Xerox.COM>
14 Dec 87 13:48:43 PST (Monday)

From the Rochester (NY) Democrat and Chronicle, Sunday Dec. 13, 1987. Without permission.

GAMBLER WHO WIRED HIMSELF TO COMPUTER FACES TRIAL

Carson City [AP] -- The [Nevada] state Supreme Court upheld a ruling against a man who wired his athletic supporter to a hidden microcomputer to improve his odds of winning at blackjack. The ruling Thursday revived a charge of possessing a cheating device that had been filed against Philip Preston Anderson in Las Vegas.

According to the court, Anderson strapped a microcomputer to his calf. Wires ran to switches in his shoes that he could tap with his toes to keep track of the cards that had been played. The computer calculated Anderson's advantage or disadvantage with the house and sent "vibratory signals to a special receiver located inside an athletic supporter," the Supreme Court said.

[The gentleman must be very well endowed. Otherwise the state Supreme Court would have declined to hear the case, on the ancient legal principle, "de minimis non curat lex." -- ARA]

Re: Expert Systems (RISKS DIGEST 5.75)

Amos Shapir <nsc!taux01!taux01.UUCP!amos@Sun.COM>
16 Dec 87 14:35:05 GMT

It seems the main problem is blindly relying on expert systems, because of lack of time and expertise. A well designed expert system should therefore give not only the answers, but also the decision path by which it got at them. A country doctor may not have all the knowledge that a hospital system provides, but may well be qualified to judge whether a decision like 'the patient has blue eyes therefore it's pneumonia' is valid in a particular case.

Amos Shapir, National Semiconductor (Israel)
6 Maskit st. P.O.B. 3007, Herzlia 46104, Israel Tel. +972 52 522261
amos%taux01@nsc.com (used to be amos%nsta@nsc.com)

The Saga of the Lost ATM Card

Scott E. Preece <preece%fang@gswd-vms.Gould.COM>
Tue, 15 Dec 87 09:26:28 CST

From: Alan Wexelblat <wex%SW.MCC.COM@MCC.COM>
> They helpfully informed me that they had no way of retreiving my card,
> but if I was willing to hang around for a while "...the machine will
> probably spit it out." ... MBank returns them cut up, you see. ...

Well, that's better than having it hand the card to the next person to use the machine, anyway. Actually, my own bank's machine swallowed my card once, for no known reason (it never even acknowledged that the card had been inserted). The bank sent me a new card and said the machine cut the card when it claimed it. In retrospect, this is probably a good idea -- the machine probably claimed the card because it couldn't read the stripe; I would imagine the probability of a read failure on a card which has already failed once is higher than on a card picked at random. So I'd rather not have a known-to-be-flakey card, anyway.

Of course, I also have a wife who has a card, so I'm easier about the time delay than if that were my only access to the system...

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

---

Telephone Billing Risks

Fred Baube <fbaube@note.nsf.gov>
Fri, 11 Dec 87 11:45:25 -0500

This is a follow-up to the article about the woman in West Germany who incorrectly returned her telephone handset to its cradle after a call to Africa, generating a phone bill of $1710 for 10 hours. It was reported here that the woman was told she could settle for one-third the amount, $570.

From _World_Weekly_News_, excerpted without permission:

"The stubborn old widow flatly refused to pay the bill. Then a judge ordered that she need only pay $570. Still she refused.

The judge threatened to toss her in the slammer.

"I said 'OK, go ahead and put me in prison,'" she declared .. " Well, that's what he did. They took me to jail .. I spent one night in jail. It was horrible .. The next day they said I could go if I would pay for only five minutes of the call.

"I said sure I would .. but not a penny more. Then I came home. But I'm still hopping mad !"

Re: F4 in 'Nam (Reversed signal polarity causing accidents)

<mnetor!utzoo!henry@uunet.UU.NET>
Thu, 10 Dec 87 13:11:29 EST

> ...the low-tech means that the pilots developed to deal with the problem...
> was to wire a pair of bayonets to the "rails" on either side of the ejection
> seat so that the points projected above the pilot's head.

There are ejection-seat systems nowadays, in fact, that rely on such "canopy

breakers" rather than using a canopy-ejection system. This does depend on having a relatively thin canopy; it wouldn't work on the thick one-piece canopies used on most new US fighters. But it's certainly simpler and more reliable than automatic canopy ejection.

Mind you, there is a negative side to having a relatively thin canopy. There was a recent accident in Britain, not yet explained in detail, which *might* have been due to the parachute-deployment system of an ejection seat firing *through* the canopy by accident (i.e. not as part of an ejection) and pulling the pilot out of the plane after it. The plane (a Harrier) unfortunately kept on flying and eventually ran out of fuel over deep ocean. Recovering it will be difficult, but may be tried because more information is badly needed.

(In case you're wondering why a parachute-deployment system should operate so violently: in an ejection at low altitude, getting the parachute out and inflated *immediately* is very important.)

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

---

For Lack of a Nut (NASDAQ Power outage) [Refinement of RISKS-5.72]

Bill McGarry <decvax!bunker!wtm@ucbvax.Berkeley.EDU>
Sun, 13 Dec 87 23:23:00 EDT

[As noted in RISKS-5.72, the NASDAQ over-the-counter computer system was knocked out of service for several hours on December 9th]. A squirrel carrying a piece of ALUMINUM FOIL made contact with some electrical equipment at a electrical substation. Although there was a power outage in the area, apparently NASDAQ suffered only a power dip (I assume that they have some form of backup power) but this power dip was enough to shut the system down [... for] over 3 1/2 hours before most services were restored.

Bill McGarry
{philabs, decvax, fortune, yale}!bunker!wtm

[Curses, FOILED again? Maybe the squirrel was hungry and went for the power DIP (which was SPIKED). (By the way, this was at least the THIRD squirrel power case noted in RISKS -- see RISKS-4.2 for two others.) PGN]

Dutch Database Privacy Laws (Re: RISKS-5.68)

Henk Cazemier <cognos!henkc@zorac.ARPA>
Thu, 10 Dec 87 12:02:41 EST

>From: Robert Stanley <roberts%cognos%math.waterloo.edu@RELAY.CS.NET>
>Subject: Dutch Database Privacy Laws
>First of all, there is the classic problem of protected software. We use Sun/3
>workstations, and the first engineering response to problems is swap out the
>processor board (our workstations are single-board). [...]

Actually, most replacement boards do NOT have an idprom when we receive them

from SUN. SUN highly recommends that you retain your original idprom, which is what we do.

Henk Cazemier P.O. Box 9707
Cognos Incorporated 3755 Riverside Dr.
VOICE: (613) 738-1440 FAX: (613) 738-0002 Ottawa, Ontario
UUCP: decvax!utzoo!dciem!nrcaer!cognos!henkc CANADA K1G 3Z4

Search RISKS using swish-e

THE RISKS DIGEST

Forum on Risks to the Public in Computers and Related Systems

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

Volume 5: Issue 77

Thursday, 17 December 1987

Contents

Lessons from a power failure

Jerome H. Saltzer <Saltzer@ATHENA.MIT.EDU>
Thu, 17 Dec 87 11:54:11 EST

About three times each year, the Cambridge Electric Company provides M.I.T. Project Athena an opportunity, at no extra charge, to check out its campus-wide power failure resiliency and cold start capability. The most recent opportunity came one week ago. We assume that Celco chose this particular time because the last week of the Fall semester has everyone (both students and Athena operations staff) stretched out about as thin as they ever get; if you are going to do a stress test why not make it really stressful?

At 11:02 a.m. on December 10 a power glitch of about a half-second duration took down 750 network workstations and 70 network servers of various types, all nominally connected in a client-server architecture, and up to that instant happily humming away doing last-minute homework assignments and final term papers. In the ensuing couple of hours we discovered two interesting things. (And of course we also learned--or I should say relearned--a half dozen less interesting things, in the same general class

as remembering to keep your fire extinguishers charged.) One of the interesting things was bad (but repairable) news, the other one was good news. Both may be of interest to designers concerned with RISKS.

First, the bad news. Our most recently introduced service is a network name service that, among other things, provides automatic lookup to determine which of 33 independent network file servers is holding your files. Although it was intended to eventually run this network name service on a set of small machines dedicated to just that purpose, we initially deployed the name service as an extra process on three of our big file servers, choosing three that were known to be lightly loaded because they also provide file backup copying service. We knew, but didn't think about, the fact that the file backup copying servers were each configured with two extra, large disk drives when compared with the other file servers.

The problem became apparent as we watched the system struggle back to its feet after the power failure. The network gateways were back on the air within a few seconds; the 15 library file servers (since they export read-only file systems) were mostly back on the air within five or ten minutes, and then the 33 file servers that hold user files began to pop to life. Within 15 to 30 minutes most of them had checked out their file systems and were ready for customers. But no customers showed up, even though almost all of the 750 workstations had dutifully rebooted themselves. The reason is that the large-configuration backup servers were still picking nits out of their three-disk file systems, and hadn't gotten to the point where they could restart the name service that everyone else depended on to figure out which file server to use. About 45 minutes into the incident, the first name server woke up, and a majority of users were back on the air, after an unnecessary delay averaging perhaps 25 minutes.

Needless to say, we are expediting the installation of the small-configuration name service hosts. RISKS lesson: The independence of dedicated servers can be one of the major benefits of a distributed server/client architecture, but the benefit is only potential till you actually get around to doing it.

The good news was the discovery that there is an extra payoff in our configuration of 33 independent, modest-sized (0.5 GB) file servers as compared with, say, 4 giant file servers. When only 31 of the 33 came back up because a water cooling pump in one machine room didn't survive the power glitch, only about 7% of our 5000 student customers were affected. And most important, we had enough spare capacity that we could consider reloading the files from the latest backup tapes of those 2 servers elsewhere. Fortunately, the cooling pump got fixed before we had to do that, but the principle has stuck in our minds. It is similar to the principle in the electric power industry that your system needs (at a minimum) spare or reserve generating capacity of about the same magnitude as the largest single generating plant in the system. RISKS lesson: The smaller the largest server, the smaller the reserve capacity you need to absorb its failure.

Jerry Saltzer

Squirrels and other pesky animals

Frank Houston <houston@nrl-csr.arpa>
Thu, 17 Dec 87 10:46:22 est

It seems to me that the problem of pests infiltrating electrical and electronic equipment is not news anymore. Recall Grace Hopper's moth.

In my youth squirrels were a common cause of power interruptions when they would climb the utility pole and try to nest in the transformer outside of our house. When I grew up and went to work in a development laboratory I saw photos of a mouse that put some test equipment out of commission by crawling inside and electrocuting itself on the power connections.
If it had happened to Eniac, we might we might be demousing, not debugging.

Frank Houston [houston@nrl-csr.arpa]

Security failures should have unlimited distributions

Andy Freeman <ANDY@Sushi.Stanford.EDU>
Thu 17 Dec 87 01:38:22-PST

Summary: Crackers already talk to each other - clearinghouses can't help them much. The only people who can benefit from clearinghouses are responsible system adminstrators. No matter how broadly clearinghouses distribute cracker techniques, it won't put systems run by irresponsible system adminstrators at any more risk than they already are.

Paul Garnet (pgarnet@csl.sri.com) writes:

> In Risks 5.71 Eugene Miya suggests
>
> < If we are ever going to progress out of the software muck, we are
> < going to have to come up with mechanisms to replace all of our
> < anecdotal information with better information.
>
> I agree. One part of the 'software muck' is illicit code, e.g., Trojan horses, viruses, etc. It is EXTREMELY difficult to obtain any examples of illicit code, as any organization which has been bitten by one of these bugs does not want to be responsible for exacerbating the situation by letting the illicit code out to possibly infect another system.
>
> The software security community needs to study the diseases which we are trying to defend against, as potential defenses created in a vacuum of information will only work in a vacuum. A clearinghouse, repository, library, or whatever name one wants to give to such a function should be set up so that those of us who are trying to build defenses can have subjects to study.
>
> There are, however, a number of sticky issues revolving about setting up such a clearinghouse.
>
> 1) How do you trust the repository? How does one know that

> information given to the repository will not be abused, nor will it be used against the giver?

If the information can be used again against the giver, it will be regardless of whether the breached site tells anyone. ("Fool me once, shame on you, fool me twice, shame on me.") The cracker still knows and crackers talk to each other.

> 2) How does the clearinghouse know who to disseminate which information to in order not to violate issue number 1? How does one decide on who has a legitimate need to see 'dangerous' information, e.g., details on viruses, trap doors, etc.

See above. The only defense comparable sites have is to find out as quickly as possible about their holes; clearinghouses should be available to everyone. A few crackers will use the clearinghouse to find out sooner than they would have otherwise, but immediate unlimited distribution gives every responsible system administrator a chance they don't have now to fix holes before cracker can slip through. Systems run by irresponsible sysadmins aren't in any more danger when everyone, not just the crackers, knows about their holes.

> 3) The clearinghouse must not be an information sink, sucking up information from anyone willing to donate their examples but never giving any information out. It must be clear that the purpose of the clearinghouse is to facilitate the sharing of information in a non-threatening way.

See above.

> 4) The clearinghouse must not be an organization that people are inherently scared of, "If I tell them what happened, what are they going to do to me?"

The clearinghouse should accept anonymous "here's how to crack operating system x", so this isn't a problem. Obviously, it shouldn't distribute anonymous solutions - the real problem is validating suggested fixes. Nevertheless, clearinghouses that do nothing but distribute "here's how to crack unix" information are valuable.

> 5) There must be some mechanism to validate the information coming to the clearinghouse to insure that it is correct. We do not want a repository of misleading, invalid data.

This is "easy" - all the clearinghouse has to do is try to crack a similar system that has is secure against all previously disclosed attacks. If it breaks, publish the new hole, otherwise let people know that if they aren't up to date, they're still vulnerable. Perhaps there should be two types of clearinghouses. One stores all holes while the second keeps track of holes that have been rereported in the past six months.

> 6) Who's going to pay for this service?

Responsible system administrators will pay for subscriptions; "evolution" will decrease the number who don't subscribe. The real problem is who is liable. Irresponsible system administrators will blame the clearinghouse even though it doesn't contribute to their insecurity. OS suppliers will be unthrilled too. Both will sue.

I think there should be competing clearinghouses. Some will specialize and may even sell fixes - they can be validated the same way any software vendor is. (Some OS vendors will run clearinghouses.) Independents will keep them honest - they'll let responsible system managers know there is a problem, and what it looks like, even if their vendor won't admit that there is one, let alone have a solution.

Many security failures are people failures. A clearinghouse will only highlight this.

-andy

2600 Magazine -- hackers, cracking systems, operating systems

Eric Corley <cmcl2!phri!dasys1!ecorley@RUTGERS.EDU>
16 Dec 87 08:55:30 GMT

There has been some talk of an article that we have published in 2600 Magazine and I wanted to make clear the reasons for our publishing such an article and what the purpose of our magazine is. The article in question is a very well documented guide to VM/CMS, run on IBM machines. It explains how the systems can be cracked, what the vulnerabilities are, and how a hacker can find what he/she is looking for. We have printed the article in two parts, the conclusion appearing in our latest issue.

2600 prints these articles because, quite frankly, people want to know these facts. Most computer hackers are not of the malicious caliber and simply explore systems to learn how they work. We find that a great many computer operators benefit greatly from the bugs and quirks that we point out.

So, in short, we aren't printing these articles on computer operating systems (UNIX, VAX, VM/CMS, VMS, etc.) and telephone systems (Sprint, MCI, AT&T, etc.) to help people break into them, NOR are we printing them to help trap computer hackers--we simply want the information to be known. Thanks for the opportunity to respond.

Eric Corley, Editor, 2600 Magazine, 2600@dasys1.UUCP, phri!dasys1!2600@nyu
(NOTICE: For those interested, 2600 is published quarterly and costs $40 for a corporate sub, $15 for individual (delivered to your home) subs. Back issues are also available. Write: 2600, PO Box 752-A, Middle Island, NY 11953. (516) 751-2600.)

Eric Corley {allegra,philabs,cmcl2}!phri\
Big Electric Cat Public Unix {bellcore,cmcl2}!cucard!dasys1!ecorley
New York, NY, USA {sun}!hoptoad/

Re: can you sue an expert system?

Roger Mann <RMann@HIS-PHOENIX-MULTICS.ARPA>
Wed, 16 Dec 87 13:09 MST

No one has asked this question yet, so I will. In the original question, the expert system was a model of a financial advisory service that gives buy, sell, and hold recommendations. The question is: can you sue a financial advisory service ? If not, then how can you sue the expert system that represents that service. If you can sue, what do advisory services do to prevent themselves from paying out gobs of money to irate customers ? Then, from that, can expert system sellers protect themselves in the same fashion ?

Re: Interchange of ATM cards

Douglas Jones <jones%cs.uiowa.edu@RELAY.CS.NET>
Wed, 16 Dec 87 09:02:52 CST

The original law requiring that all off-premise ATMs in the state accept ATM cards issued by any bank in the state was enacted in Iowa. It was immediately copied by North and South Dakota, and then by Wyoming. As a result, very soon after the introduction of ATMs, we had a 4 state uniform network (named Shazam; symbol: an S with a lightning bolt through it, making an interesting variant on the dollar sign).

Why other states have been slow to adopt this scheme is a puzzle, since the convenience to the public is so great, and the costs to the banks are so small.

The one problem with the Iowa law is that on-premise ATMs are still allowed to accept only their own brand of card, and with the public so used to free interchange of cards, mistakes at these machines can be annoying. Fortunately, the one time I was caught, the bank mailed my card to my home bank unmutilated, unlike the problems that Wexelblat described. The number of such machines that reject (or keep) foreign cards appears to be declining, probably because of the hassles they cause.

Douglas Jones

Search RISKS using swish-e

THE RISKS DIGEST

Forum on Risks to the Public in Computers and Related Systems

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

Volume 5: Issue 78

Friday, 18 December 1987

Contents

Roger Boisjoly and Ethical Behavior

<mnetor!utzoo!henry@uunet.UU.NET>
Fri, 18 Dec 87 04:41:38 EST

There has been a fair bit of back-and-forth over Roger Boisjoly et al. in private mail [subsequent to RISKS-5.63,70,71], most of which is pretty peripheral to Risks. Herewith a straight chronology of verifiable events. One or two personal notes are in brackets []. Numbers in brackets are page numbers in the Rogers report, "Report of the Presidential Commission on the Space Shuttle Challenger Accident". (Any library with any pretensions to quality should have this; it is not an obscure technical report, but a widely-distributed and not overly expensive book that is basic to real understanding of the disaster.) Quotes in single quotes are approximate, double quotes are literal.

Dramatis Personae:

B = Roger Boisjoly, Morton-Thiokol engineer
L = Bob Lund, M-T VP engineering
H = George Hardy, NASA manager
M = Larry Mulloy, NASA manager
K = Joe Kilminster, M-T VP boosters
R = Stan Reinartz, NASA manager

The scene: a teleconference between M-T Utah and two NASA centers, called to discuss the issue of cold vs. SRBs [107].

1. B: 'Don't launch.' [89] L: 'Don't launch.' [90]

2. H: 'Argh. But if contractor says don't launch, we won't.' [Note NASA willingness to at least talk about not launching.] [90]

3. K: 'If the engineers say no, M-T says no.' [90]

4. M&H: 'Argh. We think it's not that bad. We're impatient to launch.' [91-2]

5. K: 'We want a recess to talk about it.' Done. [92]

6. Much discussion. L told to put on his management hat. [93]

7. Teleconference resumes, same participants [including B]. [108]

8. K: 'Go ahead and launch.' [93] B comments later in testimony: "I did not agree with some of the statements that were being made to support the decision." [93] [Note: not just 'decision wrong' but 'supporting arguments are lies'.]

9. R asks whether anyone in the teleconference has a different position or further comments. [96,100]

10. ---> SILENCE <--- [96,100] In particular, B is silent. [93]

11. Teleconference concludes. B is unhappy but does nothing. [93]

12. Next morning: manned space program in shambles, seven astronauts dead.

13. Later, in testimony, B: "I felt I really did all I could to stop the launch." [93]

The reader will have to form his own opinions on whether Boisjoly was, in these events, a heroic whistleblower risking his job for his principles, or a dutiful company man who shut up when his management told him to shut up. He clearly did become a whistleblower later... after the damage was done.

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

---

Roger Boisjoly and Ethical Behavior

Ronni Rosenberg <ronni@CCA.CCA.COM>
Fri, 18 Dec 87 15:23:48 EST

I am afraid I continue to disagree with Henry Spencer's interpretation. It appears that he condemns Boisjoly because Boisjoly did not speak out at the teleconference after Morton Thiokol and NASA management decided to launch. But Boisjoly had argued his point vigorously at that meeting. NASA was part of the teleconference and heard these arguments; much of this is left out of the clipped, paraphrased excerpts from the Rogers report. The fact that h Boisjoly did not repeat his argument after Thiokol management clearly chose to override it hardly seems like a worthwhile basis for such harsh criticism.

Also, it is simply wrong to say that Boisjoly did not take risks before the teleconference. With the possible exception of tenured faculty, anyone who works in an organization takes a risk when criticizing management. Boisjoly did just that, repeatedly, with regard to the O-ring issue. This is not the behavior of a "dutiful company man"! Continued criticism incurs management disatisfaction, and Boisjoly increasingly was shunned and treated badly by his managers and some colleagues; yet, he kept raising the issue. The risks that he took are clear when you hear him discuss these events at length, but not when you read the "straight chronology of verifiable events" on which Spencer appears to base his entire argument. Eventually, critical behavior puts one's job on the line. Anyone who has worked at an organization should know the very real risks of being a critic.

Before the teleconference, Boisjoly took all possible action within Morton Thiokol. He complained in writing to increasingly high levels of management, up to the VP of Engineering. As a direct result, Thiokol set up a group to investigate potential problems with the O-rings. Boisjoly says the company did not assign enough resources for the group to collect adequate data. Lack of adequate resources is a common complaint. However, the procedure of setting up a group to investigate the problem was a reasonable one on the company's part. This procedure probably was a standard part of the company's structure for resolving problems, and that corporate structure had resulted in a successful shuttle program until then. Boisjoly had no reason to think that the structure would fail this time: As an engineer, he was not in a position to identify the organizational flaws that the Rogers commission later pointed out. Hence, it is not clear that he should have gone public at this time.

It was not until the teleconference -- when Boisjoly genuinely believed the launch would be delayed -- that the lack of an adequate O-ring investigation became a critical problem. It is at this point that Spencer finds fault with Boisjoly's lack of action. Yet, Boisjoly did not merely "raise doubts." He argued vigorously against launch, presenting what data he had to support his position, to both NASA and Morton Thiokol. Others made the decision. It was clear that repeating his points would not have affected the decision. He had argued his points strongly, and it appeared that NASA and Thiokol management wanted to override them.

In hindsight, it is easy to say he should have gone public at this point. But making ethical judgments in hindsight is unfair. Spencer gives Boisjoly

little credit for going public later. But without the testimony of critical, in-house engineers, the Rogers commission had little chance of discovering the truth. It was Boisjoly's perception that the commission was not getting the full story, so he risked his job and livelihood by testifying: The evidence shows that whistle-blowers are unwelcome in their own or other companies after they go public with criticism of their company.

I believe Boisjoly did everything he was ethically obligated to do, by speaking out at every available level and time to express his strong concerns and, at the end, his strong feelings against launching. By doing this, he had nothing to gain, he endured censure within the company, and he took great risks. When he later went public, he risked his job and livelihood. To say he was wrong because he did not do this earlier is to say he should have been a hero, not an average ethical human being. I think an heroic standard of behavior is unfair. While it would have been ethically right to go public earlier, I do not believe it was ethically wrong to postpone this heroic step.

Computer aids taxi dispatch

Jeff Lindorff <cae780!sequent!jeffl@sri-unix.ARPA>
Thu, 17 Dec 87 13:58:52 pst

Getting a cab in Portland, OR., may or may not be getting easier ...

(excerpted without permission from "The Oregonian")

IT'S NO LONGER CATCH AS CAB CAN -- COMPUTER SUPPLANTS RADIO DISPATCH --

Her name is Cathy, and better than anyone else she'll remember the week Broadway Cab (in Portland, OR.) got its new computers. She called the company one recent night and asked to have a particular driver call her. A message was sent over the company's brand-new computer system, but but it was inadvertently relayed not to him alone, but to the entire fleet of cabs on the road that night. She received 31 phone calls and a lesson in what happens with new computers, said Ed Stemwedel, night supervisor.

Things are changing around Broadway Cab. All 125 cabs in the company's fleet are being equipped with the small screens of a computer that will locate and assign a fare to the closest driver. The system will cost the company $500,000, and still includes radios. Drivers, after all, still need to check for special instructions. But the radios probably won't be used much.

Drivers generally seem to support the new system. It's more fair and efficient and provides good protection against "theft" of fares by other cabs, several drivers said a few days after getting the new computers. But things will be different.

There have been some problems. Two, three, even as many as six cabs have been showing up for one fare. There have been some long delays, sometimes an hour or more. And some calls are being missed altogether. But those problems are the result of human error more that anything else, said Warren Krupa, a dispatcher.

"The folks here don't know what we're doing yet" with the computers, he said. "But every day, every shift, its better. It'll take a few days."

The computer system was built by Mobile Data International of Vancouver, British Columbia. The Broadway Cab system is the only one like it on the West Coast of the United States. Vancouver, Houston, Dallas, Miami, and some New York cab companies recently have started using a similar setup, according to Denny Reed, Broadway Cab's marketing director.

Re: product liability

Martyn Thomas <mcvax!praxis!mct@uunet.UU.NET>
Thu, 17 Dec 87 17:48:56 BST

In Risks 5/73 John Gilmore writes:
<> For imported goods, the original importer into the EEC is liable.
> ..I am curious how long ... mcvax will last ... it may be the largest
>single channel for import of software.

I'm no lawyer, but I believe the liability will fall on the first company in the import chain which supplies the software as a business transaction. I believe mcvax will escape liability, though anyone importing software by this route and selling it on could be liable (under the UK Act).

> Does Lloyds of London sell bug insurance?

Yes - they are one of the largest underwriters of product liability and professional liability risks.

> It might be fun for someone to sue Praxis .....

Is this one of the RISKS of posting to this group? Anyway, we're insured, so sue away! :-)

Martyn Thomas, Praxis plc, 20 Manvers Street, Bath BA1 1PX UK.
Tel: +44-225-444700. Email: ...!uunet!mcvax!ukc!praxis!mct

Re: Expert systems liability (RISKS-5.75)

Jonathan Krueger <dgis!jkrueger@uunet.UU.NET>
Fri, 18 Dec 87 02:32:42 est

It's unreasonable to sell a product for general use when you know in advance it will mislead anyone but a specialist.

>Lawsuits are society's way of enforcing product specifications and warranties.

Aren't there some other ways? How about product testing and publication of findings, product and manufacturer reputations and their relation to repeat business or lack thereof, contractual remedies, buyer complaints and buyer/seller negotiation, and buyer preference of distributors and

middlemen who expedite resolution of buyer complaints?

Of course, these depend on the seller's interests in cooperation; there are sellers who won't cooperate. But lawsuits have their limits too. The buyer may sustain damages difficult to prove. Statutes of limitations expire. The seller may go bankrupt or skip town. He may stall. He may tie up the courts with legal maneuvering.

So neither lawsuits nor the alternatives can enforce product specifications and warranties. Not in the sense that helps an individual buyer. But, over the long run, don't suits force bad companies to shape up? In some cases. Certainly the seller will act to limit his liability; one way is to improve product quality. But there are cases where all steps have been taken long ago, when product quality is already as high as anyone knows how to make it. At that point the seller doesn't work to make his product meet the specs; he pays his last settlement and simply chooses not to sell any more.

For instance, there used to be several polio vaccine manufacturers in the U.S. Today there is only one. Probably within five years we'll import the stuff. There is no question that increased product liability caused this. The court cases are known, the history is well documented, you can add up the costs yourself. As I understand it, with the highest quality vaccine, about one in ten million kids will get a polio injection and it will kill him. A few more will experience severe side effects. Millions of kids are injected every year. Parents sue more these days. As the settlements added up, manufacturers decided one by one to leave the market.

How is the remaining U.S. vaccine manufacturer managing? Well, it raised the price to cover its losses. In no sense has it been forced to put its money where its mouth is; who do you think pays for public vaccination? The company plans to continue production as long as costs from lawsuits are predictable enough to meet with price increases.

Has the buyer been protected? Did we drive the shoddy manufacturers out of the market? No. Product quality displayed a slight negative correlation with court and settlement costs. Essentially, quality was as high as anyone could make it. It gradually improved over the years, including the years that manufacturers liability costs shot up.

Will kids enjoy a lower risk? No. Public health authorities are now arranging to buy vaccine from foreign sources when domestic is no longer available. Foreign labs can equal quality of domestic manufacturers. They can't do any better. Sometimes they do worse. But the alternative is no vaccine at all.

The simple RISKS:
  No matter what, every injection RISKS death.
  Not to inject RISKS polio for that individual.
The less simple RISKS:
  Drug manufacturers RISK getting sued.
  We all RISK a public health disaster.
The interaction RISK:

Companies take fewer RISKS to develop and sell useful drugs.

How does this apply to expert systems? By analogy. There's the RISK, well known to RISKS readers, of not using the computer. This could result from companies taking longer to develop and test the system, meanwhile perhaps the expertise it provides is less available. Or it could result from fewer companies choosing to invest in expert system development. Perhaps the entire field might advance and find acceptance and application more slowly. Is anyone willing to stand up and say that we'd be worse off if commercial and widespread use of expert systems were delayed by ten years? How about twenty? Perhaps we'd all be better off, if the software were twenty years better understood when it becomes an off-the-shelf product.

More generally, what are the trade-offs involved in driving the creation of software by fear of lawsuit? Does it motivate software companies to take longer but deliver better product when they do deliver it? How many companies will instead choose to develop less flexible, more constrained, less generally useful software? Any degree of experience with the computer field should convince one that there's satisfying amounts of money to be made offering incrementally better software at last year's prices. How often will the released product behave no more safely or correctly than it would have if we got it five years earlier, but now the product manager can tell the jury "We did five years of in-house testing!"

How many companies will make code that does little beyond covering the seller's, uh, liabilities? There are features of non-computer products out there aimed specifically at limiting liability, features which exist solely to be pointed out to juries as Safety Measures We Took. How useful will software be that follows this model?

How many companies will do what they can to develop a good product but put their faith in passing along their court and settlement costs to their customers? And how many will simply choose not to enter the market, because in our zeal to protect the buyer we left the seller a little too exposed? How many of them would otherwise create wonderful and useful systems, which like vaccines are used with risk but are better than the alternative. It's hard to evaluate this RISK. But it's there. In my opinion it argues against punitive litigation as the buyer's sole remedy and seller's chief motivation for quality.

Re: Australian telecom blackouts and 'hidden' crimes (RISKS-5.73)

Jon A. Tankersley <uunet!apctrc!cr1a!zjat02@mimsy.umd.edu>
Tue, 15 Dec 87 14:36:58 CST

In Tulsa, about 3 years ago over Thanksgiving weekend, criminals took chainsaws to the wiring boxes of the phone company to cover up other crimes. The service to about 1/3-1/2 of Tulsa was knocked out. The criminals were later caught. Unfortunately I can't seem to remember any particulars. I've been asleep a few times since then.

-tank-

Wall Street Kills The Messenger

Scot E. Wilcoxon <umn-cs!datapg.MN.ORG!sewilco@cs-gw.D.UMN.EDU>
Thu, 17 Dec 87 16:00:23 CST

"Wall Street Kills The Messenger" is an article in 'Computer & Communications DECISIONS', Dec 1987, pg 72-74,104.

The problem on Wall Street was not too much automation but rather too little. The investment strategy which most obviously failed was portfolio insurance. Portfolio insurance assumes quick trades. The weak point was not the NYSE computers but rather the interface between them and the human traders. Futures contracts trading speed was limited by the speed of printers and human traders on foot in the NYSE floor. Liquidity seemed to vanish.

Expert systems; Ejection notice? (RISKS-5.76)

Steve Philipson <steve@ames-aurora.arpa>
Thu, 17 Dec 87 13:32:34 PST

Here are some responses to a few of today's postings.

From: nsc!taux01!taux01.UUCP!amos@Sun.COM (Amos Shapir)
It seems the main problem is blindly relying on expert systems, because of lack of time and expertise. A well designed expert system should therefore give not only the answers, but also the decision path by which it got at them. A country doctor may not have all the knowledge that a hospital system provides, but may well be qualified to judge whether a decision like 'the patient has blue eyes therefore it's pneumonia' is valid in a particular case.

> This is an excellent idea, and the method should be followed whenever possible. It can't be done in all cases, though, as many expert system applications are real time, and the operator can't examine the entire decision path in the time available. For example, a pilot flying an aircraft through a fly-by-wire system can't examine all the control logic while flying the airplane. We can (and should) strive to give as much pertinent information about the decisions as possible.
>
> The NASA Aviation Safety Reporting System (ASRS) contains many reports on automated systems problems. One of particular interest concerns ground proximity warning systems. A commercial crew reported landing after a GPWS alert on approach, as they thought that the alert was erroneous. (The alert was your standard "pull-up" voice message). It turns out that the flaps were only partialy deployed and not at their correct landing setting. The GPWS could have been programmed to alert them to the specific logic rule that caused it to activate (e.g. "pull up! flaps not in landing configuration"). This might be difficult to do in practice, as

the GPWS considers many factors, and would have to be making a conclusion about the intended maneuver.

It's interesting to note that in this case the crew did not blindly follow the reccomendation of their expert system -- as far as they determined, the expert system was at fault. Who would have been judged liable if there was an accident as a result of this situation?

From: mnetor!utzoo!henry@uunet.UU.NET

>Mind you, there is a negative side to having a relatively thin canopy. There >was a recent accident in Britain, not yet explained in detail, which *might* >have been due to the parachute-deployment system of an ejection seat firing >*through* the canopy by accident (i.e. not as part of an ejection) and pulling >the pilot out of the plane after it. The plane (a Harrier) unfortunately kept >on flying and eventually ran out of fuel over deep ocean. Recovering it will >be difficult, but may be tried because more information is badly needed.

Aviation Week printed a preliminary article on this accident. It seems that the Harrier had an experimental back-up bail-out system. There had been some problems with low-altitude ejections, so this new system was devised in case the normal ejection seat did not function. It was supposed to work by firing a rocket to deploy the pilot's chute, and to release him from the ejection seat. Every ejection system has a safe deployment envelope -- it appears that the Harrier was flying faster\ than the top of this systems limit. The accident investigators have found no way that the system could have been accidently fired, and are tyring to determine if the pilot intentionally activated the system.

It seems that even emergency backup systems have their risks. These systems must also be integrated into the overall system. Perhaps for computer driven systems there should be manual (physical) interlocks hardwired in to prevent dangerous excursions from normal operation.

Steve Philipson, NASA/Ames Research Center, Moffet Field, CA

---

squirrels, mice, bugs, and Grace Hopper's moth

Mark Mandel <Mandel@BCO-MULTICS.ARPA>
Fri, 18 Dec 87 12:06 EST

The word "bug", in the sense we use in the computer world, did NOT originate with "Amazing" Grace Hopper's moth. It is attested in non-computer environments, but with the same meaning ("a mistake in design that causes errors in operation"), from before the time of the computer; certainly before the date of the log entry-with-moth. William Safire discussed this around a year ago. I've found a use in a little-known non-Tarzan novel of Edgar Rice Burroughs (_Beyond the Farthest Star_), in a context of aerodynamics or rocket design. Though the date of the book is a couple of years after Hopper's moth, the usage -- without explanation, as a colloquialism that the author assumes the

reader will understand -- is evidence that the term was already well known among engineers outside the then-nascent field of computing.

Search RISKS using swish-e

THE RISKS DIGEST

Forum on Risks to the Public in Computers and Related Systems

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

Volume 5: Issue 79

Sunday, 20 December 1987

Contents

Re: Lehigh Virus (RISKS-5.72)

"James Ford (Phantom)" <JFORD1%UA1VM.BITNET@CUNYVM.CUNY.EDU>
Fri, 18 Dec 87 15:16:33 CST

I've been reading about the PC virus that invaded Lehigh Univ. There is public domain software (2 that I know of now) that will detect potential "trojans" and/or "bombs". These programs are:

1. CHK4BOMB (check 4 bomb) - This program is used on suspected trojans.

The program will read and print the ASCII code. After that, it'll start reading the machine code. If the file writes to absolute sectors, CHK4BOMB will respond with "WARNING! THIS PROGRAM WRITES TO ABSOLUTE SECTORS! THERE IS A CHANCE THAT DATA COULD BE LOST....etc"

2. BOMBSQAD - This program is a memory resident program that will allow you to intercept READ, WRITE and VERIFY (in any combination) to your hard/floppy disks. It allow you to abort the suspected command by returning a timeout error (I think) to DOS, which gives you a ABORT, RETRY, IGNORE.....

While I can't state that it will detect ALL trojans, these "binary condoms" have detected the COMMAND.COM virus at LeHigh Univ.

Since the programs are public domain, I will gladly send them to you if you request them. If sent, the files will uploaded WITHOUT converting to EBCDIC.

James Ford, The Phantom, JFORD1@UA1VM.BITNET

IBM Xmas Prank

Fred Baube <fbaube@note.nsf.gov>
Fri, 18 Dec 87 10:03:57 -0500

From Friday's Washington Post, excerpted without permission.

"The message popped onto desktop screens in IBM offices around the country and even crossed the Atlantic and Pacific oceans, showing up in IBM outposts in West Germany, Italy and Japan."

[as pictured in the article]

```
          X
         X X
        X X X
       X X X X
      X X X X X
     X X X X X X
    X X X X X X X
       X
       X
       X
```

A very happy Christmas and my best wishes for the next year.
Let this run and enjoy yourself.
Browsing this file is no fun at all. Just type Christmas.

———

"The message that bedeviled IBM was a comparatively benevolent one and did not, as computer tricksters' creations sometimes do, destroy other material in the system .. [although] rapidly producing electronic gridlock."

"The culprit is unknown .. but preliminary investigation suggests that the message originated outside the company. IBM's mail

system is attached to those of several other institutions."

"From start to finish, the message survived only hours .."

"Does the world's biggest and most advanced computer company feel embarassed about its Christmas chain ? 'We didn't want it to happen, but we anticipated something like this might be attempted and we were prepared to deal with it.'"

Questions:
(1) An incoming message can contain an executable program, that can easily be run ?
(2) Such a message can be remailed under its contained program's control, presumably with the name of the last victim in the "From:" field ?
(3) Can IBM trace it to an originator, or was anonymity possible ?
(4) How/where can readers of RISKS submit something similar ? (strictly for professional testing purposes)
(5) Is the Internet similarly vulnerable ?

The prank seems to be benign, and therefore beneficial.
IBM seems to have dealt with it effectively (or have they ?).

Browsing this message is no fun at all. Just type Christmas ..

> [Bay Area folks can read a long front-page article by John Markoff on viruses in today's SF Chronicle-Examiner. PGN]

---

national security clearinghouse

Alan Silverstein <hpfcdt!ajs@hplabs.HP.COM>
Fri, 18 Dec 87 14:27:32 mst

> Andy Freeman, Security failures..., RISKS-5.77
> A clearinghouse, repository, library, or whatever name one wants to give
> to such a function should be set up so that those of us who are trying
> to build defenses can have subjects to study.

This falls right in the charter of the National Computer Security Center (NCSC), a federal agency. They are also the folks who evaluate Trusted Computer Systems by the Evaluation Criteria (Orange Book). Their services are "free" (tax-supported).

Alan Silverstein, Hewlett-Packard

> [We have noted this here before, but it seems worth reminding new readers that all sorts of systems have been evaluated. PGN]

Financial brokers are buying Suns...

John Gilmore <hoptoad.UUCP!gnu@cgl.ucsf.edu>

Sat, 19 Dec 87 04:26:22 PST

> In hindsight, it seems that computers on Wall Street created an
> appetite they ultimately couldn't satisfy. Following the classic
> addicts' pattern, each time investors got more powerful computers,
> they developed investment techniques that needed even more powerful
> computers....

By the way, one of the hottest new markets for Suns (and possibly other workstations) is in financial trading. A bunch of companies are doing software that lets a broker monitor a bunch more stuff, get plots of stock trends, etc, on their bitmapped Sun screen. Just being able to display N things at once in N windows will help a lot.

Today's common "quotron" terminals seem to just be dumb terminals. Well-designed support software on Suns should be able to aid brokers, the same way it has helped me to get more programming done in the same amount of time, and with higher quality.

[Wait until people figure out the nice network security flaws/features in such an environment. That will give a new meaning to INSIDER TRADING, using INSIDER COMPUTER FRAUD. PGN]

Toronto Stock Exchange Automation?

Hugh Miller <HUGH%UTORONTO.BITNET@CUNYVM.CUNY.EDU>
Sun, 20 Dec 87 14:21:03 EST

The following is excerpted without permission from "Computers-or-people dispute flares at TSE" by Fred Lebolt, *Toronto Star*, Sa 19 Dec 87, p. B1:

A dispute between floor traders and senior management at the Toronto Stock Exchange is brewing again, as the exchange studies whether computers or people should be at the center of stock market action. After what one exchange official described as a "shooting match" between the two sides, the exchange has launched a new, $1.25 million study looking into computer-based trading compared with person-to-person stock market trades.
"People's livelihoods are involved here, so tensions and anxieties are high," the official said in an interview.[...]

Newspaper photos and television clips of the stock exchange usually show the floor traders in action: often wearing brightly colored jackets, they're the ones who yell buy and sell orders on the exchange floor. At the heart of the action are the specially designated registered floor traders. This group of more than 100 individuals will guarantee to buy or sell a certain number of shares so the public will always be able to trade in those securities, and will oversee trading to make sure there's a small spread between the buy and sell prices. They have to keep tabs on all the trades in the stocks they follow.

Computer-based trading, by contrast, involves putting orders through by machine, with the buy and sell prices displayed on video terminals. The

> people behind the machines are also traders, but the deals are struck by computer keystrokes, rather than in person.[...]
>
> The controversy over computerized trading has been simmering for some time, but erupted a year ago after the exchange's board of governors approved a plan to switch two large stock issues from the trading floor to the TSE-developed Computer Assisted Trading System, known as CATS. CATS was originally introduced to handle trades in less active stocks, while major share issues remained in the hands of floor traders. The computerized system now handles almost half of the total listings on the exchange. But the news that two large stock issues were going over to CATS hit like a bombshell. Traders banded together into a Professional Traders Association to voice their concerns.
>
> What emerged was a compromise deal, in which an experimental trading area was set up using both floor traders and computer technology. But the controversy stirred up again in June, when the exchange startedpushing for a rapid expansion of the experimental trading posts throughout the floor. Many traders argued that the move was premature, and sought a postponement in the expansion, which they won.
>
> The July report [prepared for the exchange found advantages in the computer-based trading system and] reopened the controversy. [A second report, issued in September and prepared for Gordon Capital Corp., disputed much of the first report's findings. A subsequent letter sent to Toronto Stock Exchange members by Gordon Capitol president Donald Bainbridge said conclusions from the July report "were a real shock to the many experienced traders" who reviewed it.]
>
> The latest study now under way involves management, traders, and other groups. It is looking into a variety of key issues about future directions for trading and the over-all market environment.[...] When asked specifically if he believes there will be still be person-to-person trades on the exchange floor five years from now, [exchange vice-president Terry] Popowich [,who has management responsibility for floor trading,] replied, "I don't know. "I also don't know if there's going to be completely automated trading."

This is the first indication I have seen that a stock exchange is considering abandoning open outcry entirely in favour of completely on-line trading.

Previous contributions to this list have emphasized the limited role computers play in performing or influencing actual trading. It has been pointed out that they are most often utilized in margin trading, and in portfolio insurance (where, it has been hypothesized, they can contribute most to market instability during large fluctuations in share prices).

There is in this story little indication that human beings will not be at the keyboards of the new, totally on-line TSE. But the tendency in recent times has definitely been to replace human judgment with machine judgment, on the grounds that the latter is much faster and therefore able to take advantage of favorable buy/sell conditions much sooner than humans, with correspondingly greater earnings for the brokerages.

Given this tendency, are we on the way to the introduction of computer trading programs to handle trading in *ALL* stock issues? And to handle the functions previously reserved for the registered floor traders, as overseers and monitors of price spreads? And how will we insure that such enormously complex systems will not synergetically go plooey when pushed to their volume or price limits?

Hugh Miller, Department of Philosophy, University of Toronto, Toronto, Ontario., CAN M5S 1A1 (416)536-4441

<ucbcad!ames.UUCP!uunet.UU.NET!mimsy!jhu!osiris!mjr@ucbvax.Berkeley.EDU>
Sat, 19 Dec 87 12:35:20 EST

(Marcus J. Ranum)
To: KL.SRI.COM!RISKS@uunet.uu.net
Subject: Who Sues? (Re: RISKS DIGEST 5.75)

It would be nice to think that the current trend towards suing anyone and everything in the near vicinity of a mistake does not indicate that Americans are not losing track of the basic principles of causality !!

Can't anyone take credit for their own mistakes anymore ? If someone wishes to place their trust in an ES, and it turns out to be misplaced, I'd look at "assigning the blame" as follows:

Person who did not exercise common sense: 99.5%
Programmer who marketted malfun software: 00.4%
Assembly of chips and magnetic oxide: 00.1%

Until it is a fact of reality that expert systems are KNOWN to be reliable, then a person is unreasonable in trying to sue the producer of a product that common sense would indicate as potentially unreliable.

I understand that these views have no weight against current "law" and "legal" decisions. On the other hand, our legal system is becoming less and less a system of justice and common sense, and more and more a self-feeding system of self-reproducing rules...

It concerns me that nobody can stand up anymore and say "wow, I goofed" or "I should have used my own !@#!@#!@# brain instead of flipping a coin" when something goes wrong and they are associated with it. I can see a case where an airplane crashes because of poor service as the fault of the airline. There must, however, be a provision for acts of god, or a simple admission of stupidity.

An elderly woman recently won a lawsuit against a soda bottler because her eye was hurt when a cap hit it. She was taking the cap off the bottle with pliers, and the pliers slipped. Essentially, the "law" and the "lawyers" are saying that it is permissible (even rewarded) to be stupid.

--mjr();

The Fable of the Computer that Made Something

Geraint Jones <geraint%prg.oxford.ac.uk@NSS.Cs.Ucl.AC.UK>
Sat, 19 Dec 87 14:21:15 GMT

It has happened before, but is worth documenting that almost all the media here reported the last year's erroneous calculations of the Retail Price Index as a computer error. It was the BBC's flagship evening radio news bulletin on Friday that I heard report that ``a computer made a mistake''. As far as I can see, this time it was not even the case that `the computer' was incorrectly instructed; rather it was decided to perform an (almost) entirely unrelated calculation, and it just so happened that a computer was used to do the adding up. Using a computer means never having to say sorry. gj

---

Re: Litigation over an expert system

Rich <RMRichardson.PA@Xerox.COM>
18 Dec 87 21:18:46 PST (Friday)

> In Risks digest 5.71, chapman@russell.stanford.edu (Gary Chapman)
> mentions a "goofy" California law that provides for a defendant who
> is only 1% responsible to pay 1% of the judgement. Although this
> law may be goofy, it is a major improvement over previous versions. ...

I think the new law applies to "punitive damages" and real damages (actual loss) may still be taken from any of the "deep pocket" defendants. Am I wrong?

Rich

Tulsa; Bugs (Re: RISKS-5.78)

99700000 <haynes@ucscc.UCSC.EDU>
Sat, 19 Dec 87 00:07:53 PST

1) RE the Tulsa event of criminals sawing up telephone boxes. Here in Santa Cruz a few weeks ago transients living under a bridge built a fire to keep warm - right on top of a nest of conduits carrying telephone cables!

2) RE "Bug" - I remember vaguely reading some boys' book of the 1920s (something like Tom Swift) in which one of the characters is working on his invention and says he just has to get a few bugs out before it will work right.

haynes@ucscc.bitnet, ...ucbvax!ucscc!haynes, ...

More ATM information

George Bray <lcc.ghb@SEAS.UCLA.EDU>
Thu, 17 Dec 87 19:33:54 PST

We have discussed several issues of ATMs recently, and I want to add a few more nuggets:

1. Recently, a contributor mentioned that their bank claimed that "the ATM cuts the card if there is something wrong with it." I have experience with ATMs made by IBM, Docutel and Diebold (and various Diebold emulators) and none of them cut the card when capturing it. It is simply stacked inside the machine.

   Typically, bank tellers do cut the cards up after removing them from the machine, but that is done by a person, not by the ATM.

2. Another contributor mentioned that banks don't wish to discuss their systems, even when they implement standards that are publicly available. This is quite true in my experience. The manufacturers of bank hardware and the banks themselves depend mostly upon ignorance for protection.

3. Most bank transaction security is aimed at preventing losses to the bank, not to the cardholder. In fact, ATM security isn't seen as a big problem, because even with a stolen card, the most a burglar could get away with is a few hundred dollars at a time. (Again, tough on the poor customer, but it is cheap for the bank to eat the loss if the customer complains).

   In fact, the prevailing attitude is that the major threat to ATMs is physical: since there is about $40,000 in a fully-loaded ATM, but it will only dispense a maximum of a few dozen bills at a time, the easiest way to get money out is to blow the front off the ATM, or attack it with a car, etc.

4. As an aside, it is interesting that in many cases bank regulations have not caught up with the concept of ATMs. In California at least, the banking laws stipulate that any location that accepts deposits for a bank must be a branch of that bank. This means that ATMs owned by a different bank can't be used for deposits, even if the data processing and money handling for the two banks are run by the same data processing provider.

   This regulation becomes onerous when combined with the definition of a transfer: "a withdrawal from one account followed by a deposit to another account". This means that one is not allowed by law to press a button on an ATM commanding a computer to transfer funds between two accounts which consist of bits on a disk drive connected to that computer.

George Bray

Truncation (Doug Mosher, Re: RISKS-5.69)

Alex Heatley <alex@comp.vuw.ac.nz>
Tue, 8 Dec 87 15:24:43 +1300

> It is ALWAYS BAD PRACTICE to truncate anything without notice.
>
>Many examples over the years occur to me; here's a small partial list.

Regarding VM/CMS (IBM Mainframe OS) here's a nasty one that has caught me twice. When you change your password you are allowed to enter one that is longer than 8 characters. However, upon logging in, your password is truncated to 8 characters. The OS goes away and compares the entered password with the one in the file (passwords are kept in clear in a special file that only the SYSADMIN is supposed to be able to access -- ha!) aha! it says these are not equivalent and refuses to let you log in.

Now you know that you typed in the right password so you try again but, after five attempts the OS will lock you out of the terminal. So you walk away in confusion. If the terminal is in a public place, eventually, another user will try to use the terminal -- and will receive the error message that they can't login -- yes that's right the OS locks the terminal from being used until either the SYSADMIN resets it or n (SYSADMIN defined) hours have elapsed.

Aren't IBM OS's fun!!!

Alex Heatley : CSC, Victoria University of Wellington, New Zealand.
Domain: alex@comp.vuw.ac.nz Path: ...!uunet!vuwcomp!alex

Search RISKS using swish-e

Report problems with the web pages to the maintainer

Search RISKS using swish-e

THE RISKS DIGEST

Forum on Risks to the Public in Computers and Related Systems

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

Volume 5: Issue 80

Monday, 21 December 1987

Contents

Re: IBM Christmas Virus

Ross Patterson <A024012%RUTVM1.BITNET@CUNYVM.CUNY.EDU>
Mon, 21 Dec 87 15:22:26 EST

There have been several messages to RISKS lately about the CHRISTMAs EXEC virus on IBM's network. This was an extension of the same problem on BITNET and its European counterpart, EARN. Since I raised the general alarm about it, I'd like to answer a few questions.

The virus used two standard CMS files, called NAMES and NETLOG, to help it infect other users. The NAMES file contains a list of userids and system names that you correspond with frequently, allowing you to abbreviate them to a mnemonic nickname when sending mail, files, or interactive messages. I composed this mail by sending to "RISKS", which my NAMES file lists as user RISKS on system KL.SRI.COM. You can also list phone numbers, paper addresses, etc. There is a commonly available program that will print off a personal phonebook from your NAMES file ("Traveling Sidekick" from the days BB - Before Borland). The NETLOG file lists all users you've sent mail or files to, or

received them from. It's a very nice audit trail when you're trying to remember where you got that copy of Space Wars.

After typing the Christmas Tree on your terminal, the virus proceeded to read both the NAMES and NETLOG files to get a set of target addresses. It then sent a copy of itself to each of them, and finally deleted itself.

>From: davy@intrepid.ecn.purdue.edu (Dave Curry)
>Subject: IBM invaded by a Christmas virus {RISKS 5.72}
> ...
>This article seems to have a lot of things in it that the reporter didn't
>understand. I assume that the "terminals" in question are really PC's
>connected to the mainframes; for one thing.

The terminals mentioned are generally IBM 3270's, and PC's with IRMA-type cards. The virus ran on the host system, not on the PC.

> Plus, I presume the "Don't
>browse it" refers to the VM/CMS "BROWSE" command used for looking through
>files, and not just to the regular English word.

Both, actually. The intent was obviously to stop the reader from going further down into the file, where the real purpose of the program was quite obvious. The language used (IBM's REXX) is usually interpreted, so the program was sent in source form. Anyone who bothered to read below the second screen-full (like all of us paranoid Systems Programmers) began to see the trouble. It was slightly cloudy, as all the variable names were in German, but seeing was fair to good.

>Subject: IBM Xmas Prank {RISKS 5.79}
>From: Fred Baube <fbaube@note.nsf.gov>
> ...
>"The culprit is unknown

That is no longer the case. The culprit has been tracked down, and barred from access to his/her system. A note to that effect was broadcast to a number of mailing lists by the General Secretary of EARN. The source system had recently been attached to the West German section of EARN, and the user who started it all only intended to send a greeting to a few friends. To quote a TV commerical, "... and they'll tell two friends, and so on, and so on, ...".

> .. but preliminary investigation suggests
>that the message originated outside the company. IBM's mail
>system is attached to those of several other institutions."

Quite so. No one seems quite sure which of the gateways between BITNET/EARN and IBM's internal network, VNET, passed the first copy of the virus. It matters very little, since it found the VNET environment even more conducive to reproduction than BITNET/EARN. VNET'ers apparently keep much larger NAMES files than BITNET'ers. It wasn't long before the links were carrying more CHRISTMA EXEC's than

anything else.

>"From start to finish, the message survived only hours .."

Per copy, perhaps. The first known instance of infection was at about 1300 GMT on Wednesday, December 9. Within BITNET, it was generally stamped out by the following Monday, December 14. On VNET, it didn't show up until a day later, and was mostly killed in a massive network shutdown on Friday.

>...
>Questions:
>(1) An incoming message can contain an executable program,
> that can easily be run ?

Yes. Please remember that the Internet is not the only network style in the world. In BITNET and VNET, mail is just another case of file transfer. File transfer is performed by the sender, not the receiver. These are store-and-forward networks, so the path from system A to system B need not be intact for the duration of the transfer. The viral program was transferred as a normal file, not as mail.

>(2) Such a message can be remailed under its contained program's
> control, presumably with the name of the last victim in the
> "From:" field ?

It wasn't mailed. Thus, there wasn't any From: field, etc. It did carry the system name and userid of the most recent victim, but not any trace-back information.

>(3) Can IBM trace it to an originator, or was anonymity possible ?

A task force of BITNET and EARN systems programmers traced it back to its source, by the usual disease-control procedures:

Doctor: "Miss X, you've got a nasty case of viral <Y>. Who have you had contact with recently?".

Miss X: "Just a moment, I'll check my notebook."

A byproduct of the tool used to transmit the virus is an entry in the NETLOG file listing the userid and system name of anyone it was sent to, making it easier than usual for Miss X to remember. In some cases, the user had suppressed the NETLOG facility, but that is the exception, not the rule.

>(4) How/where can readers of RISKS submit something similar ?
> (strictly for professional testing purposes)

Noplace safely. Please don't try it on anything but an isolated network, and then coldstart your spool afterwards.

>(5) Is the Internet similarly vulnerable ?

Not to this one. It plays on several things that the Internet doesn't have:

1) A large number of IBM VM/CMS systems. The program would only run in a CMS environment. There is no reason one couldn't write something similar in any other language, though.

2) A suitable file transfer system. FTP doesn't apply. It must provide a way for a user to receive an unsolicited file, in a runnable form.

3) A good method of determining targets. The CMS NAMES and NETLOG files provided an excellent source of information. I suppose in a Unix environment, ".alias" and "/etc/aliases" would be ok, but .alias is comparatively rare, while NAMES files are almost universal in CMS.

>The prank seems to be benign, and therefore beneficial.

That is being debated in several circles. I, for one, agree with you.

>IBM seems to have dealt with it effectively (or have they ?).

Yes, they have.

>Browsing this message is no fun at all. Just type Christmas ..

The lesson of this one is the same as for PC viruses: Never run something you don't recognize. When the virus first appeared, several people suggested that it was the work of students, and that it might be used negatively in an ongoing argument over whether students belong on BITNET. When we heard that "professionals" inside IBM were also running programs they didn't recognize, that particular suggestion vanished.

This virus was quite sly, in that by sending itself to people listed in your NAMES and NETLOG files, those people would recognize the source (you) as a friend, and be generally less inquisitive, until things got nasty. Lesson #2: Even your friends sometimes make mistakes.

Ross Patterson, Rutgers University

[RISKS received an unusually large number of messages on this subject -- from Fred Baube, John Owens (2), Allan Pratt, Anne Louise Gockel, and Bruce O'Neel. I started trying to edit them down, but rapidly gave up that strategy -- inordinate overlap. So, I will take a new tack, which is to put out Ross' message -- which was the most comprehensive -- and then give Fred, John, Allan, Anne and Bruce first priority if THEY wish to comment marginally or additionally thereupon. Please be terse -- and avoid replicating ALL of the foregoing text in your messages, as some of you have been doing. (One of the joys of mailers?) PGN]

Logic Bomb case thrown out of court

<"ZZASSGL" <ZZASSGL@CMS.UMRCC.AC.UK> [Presumably Geoff Lane]>
Mon, 21 Dec 87 16:03:05 GMT

As I have not seen anything about this in RISKs yet ... The case brought against James McMahon, who was accused of placing logic bombs within the computer system used by Pandair Freight, has been thrown out of court because of "unsatisfactory evidence". The judge has ruled that there was no case to answer. This was reported in Computer Weekly dated December 17/24, 1987.

It will be interesting to learn in what way the evidence was unsatisfactory. There used to be a problem in British law(and it may still exist) in that evidence could only be given by humans. Information generated by a computer without the explicit involvement of a human could not be used in court. I may have got this legal point garbled as I don't speak legalese.

Geoff, UMRCC

Repository for Illicit Code

Steve Jong/NaC Pubs <jong%delni.DEC@decwrl.dec.com>
21 Dec 87 16:23

If there is a legitimate need to study illicit code such as viruses and embezzlement routines, and not just a forensic need to try and track down the author, then there could indeed by a need for a repository. I suggest the model of the Center for Disease Control in Atlanta, which has samples of pathogens. However, note that there was (is?) a controversy surrounding CDC's wish to keep samples of smallpox, which, it is believed, has otherwise been eradicated from the face of the earth. Why leave one known source?

Personally, I'd just as soon not have the code samples around. I'd just be tempted to play with them. (Disclaimer: I'm not a programmer.)

[Program viruses, Trojan horses, etc., will never be competely eradicated. They tend to re-erupt spontaneously or be rediscovered. PGN]

Roger Boisjoly and Ethical Behavior

<Stuart_Freedman@BKR.CEO.DG.COM>
Mon, 21 Dec 87 13:20:18 EST

To add my $0.02 to the conversation on Roger Boisjoly, I agree with Ronni Rosenberg, having seen a videotape of him telling his story. I seem to recall that he made reference to the same period of silence (the last time anyone called for objections to the launch) that Henry Spencer did. Boisjoly said that he was much too astonished at the decision to go through with the

launch (despite his strong objections) to say anything at that point. He did not fully recover his senses until after the teleconference ended. I think that we can only expect the man to be human; we can't always act heroically when we're in shock...

Stuart Freedman stuart@bkr.ceo.dg.com or rti!xyzzy!freedman@mcnc.org
Data General Corp.(Mail Stop E-219), Westboro, MA 01580 +1(617)870-9659
Pick an e-mail address -- any e-mail address...

Truncation and VM passwords

jcmorris@mitre.arpa <Joe Morris>
Mon, 21 Dec 87 10:24:46 EST

In RISKS 5:79 Alex Heatley reports that he can establish a password of more than eight characters in the IBM VM system, but that on login the system truncates the entered password to eight characters, then (correctly) reports that it fails to match the one in the access control file.

I don't know what security system his system uses, but IBM's DIRMAINT product, which is probably the most widely used directory maintenance facility used in VM installations, refuses to accept an oversized password. I just tried to enter one on our system, and was rebuffed with message DVHDIR017E.

Joe Morris (jcmorris@mitre.ARPA)

competing ATM networks

Chris Koenigsberg <ckk+@andrew.cmu.edu>
Sun, 20 Dec 87 22:22:24 -0500 (EST)

The two competing local ATM cards in Pennsylvania are Cashstream and MAC. All the Pittsburgh banks with ATM cards are signed up for one or the other local networks. Cashstream is run mainly by Mellon Bank, MAC mainly by Pgh. National Bank. Both Cashstream and MAC extend into neighboring states. Meanwhile Cashstream is hooked up with the national ATM network called CIRRUS, while MAC is part of the national PLUS system.

I've used my Cashstream card in CIRRUS machines in other faraway states, and I've used my MAC card in PLUS machines across the country. But I always assumed that these two kinds of cards were big competitors at each level : bank vs. bank, local net vs. local net, and national vs. national, and that the two sides wouldn't cross.

But in New York, there are ATM machines which accept both MAC and Cirrus cards. I was surprised, since in Pennsylvania, MAC cards work in PLUS machines but not in Cirrus machines, as MAC's local competitor Cashstream is connected with Cirrus.

Search RISKS using swish-e

Report problems with the web pages to the maintainer

Search RISKS using swish-e

THE RISKS DIGEST

Forum on Risks to the Public in Computers and Related Systems

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

Volume 5: Issue 81

Tuesday, 22 December 1987

Contents

The Christmas Card Caper, (hopefully) concluded

Joe Morris (jcmorris@mitre.arpa) <jcmorris@mitre.arpa>
Mon, 21 Dec 87 11:45:03 EST

The following item was posted on the VMSHARE bulletin board. It describes the origin of the CHRISTMAS EXEC file, and makes valid points about the inability of computer systems to automatically recognize some types of ill-behaved programs quickly enough to prevent damage to a network.

(VMSHARE is a closed bulletin board operated for the use of VM installations who are members of SHARE, the large IBM mainframe user group. Shadow copies of the VMSHARE traffic are distributed to many other nets, including VNET and BITNET.)

Joe Morris (jcmorris@mitre)

Append on 12/19/87 at 20:10 by Melinda Varian <BITNET: MAINT@PUCC>:

The following statement, from a member of the EARN Board, answers the queries about the origin of the CHRISTMA EXEC. Clausthal-Zellerfeld is quite a new VM installation. When Heinz Haunhorst, of their staff, was notified that the first appearances of the virus on the networks originated at his node, he pursued the matter vigorously and skillfully. Helmut Woehlbier, of the Technical University of Braunschweig, also did an excellent job in helping to determine the originating node.

<> <> <> <> <> <> <> <> <> <> <> <> <> <> <> <> <> <>

Date: Wed, 16 Dec 87 18:33:58 GMT
Sender: EARN Technical Group <EARNTECH@EB0UB011>
From: Michael Hebgen <$02@DHDURZ1>
Comments: To: EARN Executive <EARNEXEC@IRLEARN>,
EARN Board of Directors <EARN-BOD@IRLEARN>
Comments: cc: German EARN Executive <DEARNEX@DHDURZ1>,
German EARN node administrators <DEARNADM@DEARN>,
Heinz Haunhorst <HENRY@DCZTU1>,
"Dr. Gerald Lange" <LANGE@DCZTU1>,
Otto Bernd Kirchner <KIRCHNER@DS0IBM1>
To: Melinda Varian <MAINT@PUCC>
Subject: CHRISTMAS EXEC

Dear colleagues,

after some very sophisticated detective work it is clear that the origin of the CHRISTMAS EXEC is the EARN node DCZTU1. A student there has written this EXEC to send christmas greetings to his colleagues and another student has used it without knowing what he is doing (as many of our network users) and started the explosion.

The node DCZTU1 has already blocked the Userid of the author and done all necessary steps. Every node in the network can be the next starting point of a similar explosion and distribute virus programms or other bad things.

As far as I know the EDP-systems there is no way to prevent users from their own mistakes. The only solution I can think of for this type of behaviour is to observe "EDP-hygiene":

> If you receive an executable file (EXEC, CLIST, program) from another might be unknown user do N O T execute without control because it can result in gross missdemanour and serious damage.
>
> Check all EXECs/CLISTs, what they are doing, before you execute them and check all executable programs, where they come from and what they do.
>
> As in normal life uncontrolled behaviour may result in serious

consequences (I am not going to mention AIDS). You as a user are responsable for all what you are doing.

I propose to include such statements (in better english formulation) into the CODE OF CONDUCT and to start an "enlightenment" process for the end-users

Best regards, m[e]rry christmas (without tree) and a happy new year

Michael Hebgen

EARN director of Germany and
General secretary of EARN

*** APPENDED 12/19/87 20:10:47 BY PU/MELINDA ***

ADDED NOTE FROM JOE MORRIS:

Did any contributor suggest how the message jumped from EARN (or BITNET) into VNET? Supposedly the gateways (one at Yorktown, I believe) are monitored closely so that the ability of a message to cross without supervision is quite limited. I'm told that a few years ago there was something of a major flap when a meeting of relatively high IBM brass was shown a message Melinda Varian (the BITNET source of the EARN message I forwarded) had sent to an IBM'er via VNET (WITH the permission of IBM...upper management in IBM just hadn't been aware of the arrangement). My guess would be that it came through an account on a customer machine but assigned to an IBM'er who could pass mail into the IBM network.

Thought for the week: was this supposed to be a demonstration of a computerized Christmas distribution TREE?

Second thought on the word "tree" (swiped from an undergraduate thesis at MIT from the 60's):

Problems are posed by fools like me,
but only heuristics can search a tree.

Joe Morris

The Virus of Christmas Past (Re: RISKS-5.80)

Una Smith <0402909%pucc.bitnet@RUTGERS.EDU>
Tue, 22 Dec 87 13:32:07 EST

Re the discussion of receiving run-able mail files (sometimes viruses) via BITNET.

A few years ago I received 2 pieces of mail, an XMAS EXEC written in EXEC2 and a compiled module of some sort. The module was hard to break into, so no one I knew then knew how to tell what it did without running

it. Well, it was a very nice, benign bug:

First, it imitated all the usual system messages one gets when logging off, up to the full-screen VM370 logo. Then, slowly, the logo disintegrated into a night time scene of a cottage on a snowy hillside under some pine trees, smoke floating out of the chimney (the "smoke" was made up of phrases; "s..m..o..k..e" and "M..e..r..r..y...C..h..r..i..s..t..m..a..s", etc.), and snow flakes "*" falling from the sky. Elapsed time: about 5 minutes. Then it quit, abruptly leaving you sitting in front of a terminal in some dingy office or terminal room, just as you were before.

The clue to this so-called Christmas card's origin was that the usual machine name in the lower right was replaced with, if I remember correctly, PSUVM. Has anyone on the net now got an old copy of that somewhere? I didn't keep mine.

---

viruses and "anti-bodies"

<kahle@Think.COM>
Tue, 22 Dec 87 10:19:32 EST

Risks, recently, has been filled with reports of specific virus and how to kill them manually. Has there been any work on "anti-bodies" that attack specific viruses? It seems that contributors have enough knowledge about each virus to build such beasts. Such programs might push the state of the art, reduce the effect of viruses, and keep down the traffic on this list.

-brewster

[A certain amount can be done contextually, e.g., with specific file names. Paul Karger has suggested something similar for Trojan horses. See his paper in the 1987 IEEE Symposium on Security and Privacy. But such techniques are intrinsically incomplete. PGN]

Cleaning Your PC Can Be Hazardous to Your Health

Brian M. Clapper <clapper@nadc.arpa>
Tue, 22 Dec 87 09:57:26 EST

The following news bulletin appeared on our mail machine this morning:

"Recently a flash fire occurred at a Navy lab when an employee attempted to clean his computer screen using an alcohol based cleaner. An investigation revealed that the employee sprayed the cleaner directly at the unit while it was turned on. Static electricity which had built up on the screen then ignited the atomized cleaner. To prevent a similar occurrence here, all PC users are cautioned to turn off their screens before cleaning, and to dampen a cloth with the cleaner before wiping the screen rather than spraying it at the screen."

Brian M. Clapper, Naval Air Development Center, Warminster, PA 18976

Product liability

<fulk@cs.rochester.edu>
Mon, 21 Dec 87 11:24:30 EST

It seems to me that a large number of problems with product liability arise from a propensity to confuse two issues: _liability_ and _negligence_.

If the use of a product carries with it a certain, irreducible risk of injury, then the manufacturer SHOULD be liable for the damages resulting. That liability SHOULD result in increased costs to the users of the product (or to the public in general, in the case of mass vaccines). After all, the damages are part of the cost of the product. Such a liability should be limited to actual damages, meaning such things as medical costs, loss of earning power, and _reasonable_ (capped) compensation for pain and suffering. In particular, _punitive_ damages should be reserved for cases of negligence. Part of the result is that this sort of liability ought to result in predictable costs to the manufacturer, so that it can include those costs in the final price. Finally, most such liability cases should be resolved in administrative courts with low legal costs and short delays.

Cases of negligence arise when someone fails to take reasonable and prudent care; for example, the Ford Pinto sort of case. In such cases the present system is perfectly reasonable, with contingency fees and the like. I would not want to see lawyer's fees fixed for such cases, as I believe that would deny legal protection to the poor and would prevent pursuit of cases against the largest and wealthiest defendants. If, as is often asserted, manufacturers are wrongly found negligent because a jury wants to compensate some obviously suffering individual, then the compensation under the liability-no-negligence system should satisfy the jury's desires.

Such a system requires specifying a number of special cases; for example, if a corporation buys an expert system, they presumably have access to someone who can explain the risks inherent in using that system. In such cases, sharp limits on non-negligent liability are reasonable. It would not be the author's fault if the company managed the entire pension fund with his financial system.

In general, if we were to shift to such a split system of liability, it would take us quite a while and quite a bit of experience to develop the details. Finally, I would like to add that this idea is not original with me; I first saw it advocated in an editorial in Nature.

Mark A. Fulk
fulk@cs.rochester.edu

P.S. This is not to say that government-imposed fines and the like are not also appropriate. They are simply insufficient, as the government frequently lacks the stomach to take on offenders. The tort system provides a channel for citizen-originated complaints to get a hearing in front of disinterested parties.

Squirrels, mice, bugs, and Grace Hopper's moth (Re: RISKS-5.78)

Peter Mabey <mcvax!stl.stc.co.uk!phm@uunet.UU.NET>
Mon, 21 Dec 87 16:13:24 GMT

> Squirrels, mice, bugs, and Grace Hopper's moth (Mark Mandel) ...
>
>The word "bug", in the sense we use in the computer world, did NOT
>originate with "Amazing" Grace Hopper's moth. ...

According to the Oxford English Dictionary (Supplement I), the first recorded use of the term in print is a quote from Edison in the Pall Mall Gazette of 1889 - so it's probably coming up to its centenary now.

Peter Mabey (phm@stl ...!mcvax!ukc!stl!phm +44-279-29531 x3596)
Standard Technology Ltd., London Road, Harlow, Essex CM17 9NA, U.K.

Fire at O'Hare (Computerworld, Dec 14 issue)

99700000 <haynes@ucscc.UCSC.EDU>
Tue, 22 Dec 87 11:45:25 PST

Has an article about another fire resulting in melted cables, this time a fire at O'Hare that put United Airlines out of operation.

And has a special section on computer security. No better than one would expect from Computerworld, but that's it.

American Express computer problem

Frank Wales <mcvax!zen.co.uk!frank@uunet.UU.NET>
Fri, 18 Dec 87 17:23:52 GMT

You may be interested in a letter I received this morning from American Express; its text is as follows:

[the letter is verbatim -- the poor grammar is theirs, not mine]

Dear Mr Wales

I regret to advise you that a problem has arisen concerning access to our Automated Teller Machine network.

As you know a Personal Identification Number (PIN) is needed to use these machines. Due to an internal system error your unique PIN has been deleted. The effect of which, is to deny you access to cash or Travellers Cheque withdrawal. Would you please call London (01) [...] or Brighton [...]
where our staff will immediately amend our records with the PIN of your choice. When telephoning, please be prepared to answer

two or three questions about your personal details so that we
can maintain the necessary security.

I am very sorry for the inconvenience this must cause.

Yours sincerely
(signed by Xerox)
N.Colwell
Director
Customer Services

[I have deleted the telephone numbers above, for obvious reasons. PGN]

First of all, because the numbers are not normal customer service numbers, I called the 24-hour Emergency number (the normal Customer Service number was busy, as usual), and made sure that the letter was not a scam. I was told, after some rummaging around by the operator, that both were legitimate Amex numbers. I then called the London one, and found that, according to the exchange, it didn't exist. I then called the Brighton one and, after being asked to hold for so long that the operator had to physically go and get her supervisor, sorted out my PIN with them.

In the course of this, I asked what had happened: (I'm paraphrasing here -- it was an hour ago)

Amex: "A slight computer problem; nothing to worry about."

Me: "You mean you've had a security breach?"

Amex: "No, no. Nothing like that. That's impossible. Our systems are completely confidential. Someone was just transferring some information onto one of our systems, to make it more efficient, you know, and some information got deleted in the process. We didn't even know until members started calling us up to ask why their cards were being rejected by dispensers."

I didn't ask where their backups were -- they obviously didn't have any, or they wouldn't have been reduced to admitting their failure to their customers.

Aside from Amex's dubious practice of actually asking customers to write down a PIN and post it to them (or, in this case, tell them over the phone), something which both astonishes and amuses my Bank Manager, what does this episode reveal about American Express's computer systems and procedures, often touted as being among the best in the banking business?

[As a side note, I'm also not too convinced that the questions about personal details are good enough to convince them that I am who I say I am; I know that the information I gave wouldn't convince *me*. But that's an issue for another day.]

Frank Wales, Development Engineer, [frank@zen.uucp<->mcvax!zen.co.uk!frank]
Zengrange Ltd., Greenfield Rd., Leeds, ENGLAND, LS9 8DB. (+44) 532 489048 x220

NYT article on computers in stock crash

Hal Perkins <hal@gvax.cs.cornell.edu>
Mon, 21 Dec 87 21:48:36 EST

[Last week the New York Times ran a series of articles analyzing the stock market crash. One was on the role of computers in the crash. It's too long to include the whole thing in Risks. These excerpts concentrate on the unplanned and unexpected and omit background information about program trading, etc. I highly recommend the entire article to anyone who is interested in the subject. It also is good holiday reading for any Star Wars fans who believe that computers can be programmed to direct a real-time battle successfully. HP]

From The New York Times, Tuesday, December 15, 1987. Page 1.

The Computer's Contribution to the Rise and Fall of Stocks
by David E. Sanger

In the span of a few hours, the stock market's October collapse drove home the fact that new technology has done far more to Wall Street than just accelerate the tempo of trading.

Securities firms have always embraced innovations that promised to improve their profits. During this decade... brokerages spent millions of dollars on electronic networks... [and on] complex computerized trading techniques to exploit the flood of information.

But in the process, the new generation of hardware and software fundamentally altered the way buying and selling decisions were made. And they subtly magnified the degree of risk that investors and traders routinely accepted.

... [B]ig investors, seeking an advantage measured in seconds, were often led to abandon independent judgement in favor of executing trading strategies programmed into their computers.

On Monday, Oct. 19, Wall Street's legendary herd instincts, now embedded in digital code and amplified by hundreds of computers, helped turn a selloff into a panic....

"We are learning that when we compress the time in which things happen, they happen differently," said Robert A. Brusca, the chief economist at Nikko Securities....

[Discussion of how the technology fueled the willingness of big investors to trade for short-term profit instead of investing for long-term returns.] In other words, it helped turn [large, traditionally conservative institutions] from investors into traders.

What's more, the computer's enormous appetite for price data helped divorce buy and sell decisions from developments in the business world,

focusing them instead on numerical relationships among thousands of fluctuating stock prices....

Technology also gave a false sense of security to investors who deceived themselves into thinking that ballyhooed computer-based trading techniques would somehow protect them in a falling market....

The Allure of Technology

[Discussion of how the stock exchanges have built huge computer centers to process enormous daily transaction volumes.]

Starting six years ago, a new generation of personal computers and more powerful work stations began playing another, very different role... They were programmed to spot bargains, and to constantly compare the prices of stock index futures contracts... with the prices of the actual stocks....

Without question the new techniques made the markets more efficient... [assuring] that prices reflected pertinent information instantly, and they encouraged investors to trade simultaneously in more than one market, helping to minimize disparities in prices.

But the programs also introduced enormous pressure to act and react instantly. "Overnight, the reaction time to market-influencing events dropped from months or days to minutes and seconds," said Allen Sinai, the chief economist of Sherson Lehman Brothers. "Unless you could evaluate all this data instantly, you were out of business."

New Tricks for Investors

[Description of various "program trading" strategies, including stock index arbitrage, which takes advantage of momentary differences between the prices of stocks and of the corresponding futures contracts (trades must be made instantly before the price difference disappears), and portfolio insurance, which is supposed to reduce the risk of a downturn by selling stock index futures.]

[on portfolio insurance:] Advocates of the system were asserting before the collapse that it assured that losses would not exceed 5 percent of the value of the portfolio....

Promotions [of portfolio insurance] worked: By October, between $70 billion and $90 billion was invested in funds using some form of the insurance....

As a result, some [investors] abandoned ordinary prudent techniques, such as selling a portion of their holdings for cash when the market hit new highs, because they were confident the programs would work....

When Facts Became Myths

The problems lay in the computerized models of how markets act: They rested on assumptions that proved false. One assumption, for example,

was that the markets would be well behaved, meaning that stock prices and futures prices would closely track each other. Another was that whenever the computer commanded a buy or a sell, there would be buyers and sellers.

On Oct. 19, neither condition applied. Stocks and futures prices were far out of whack. At times, no buyers could be found. Computers literally froze -- they were not programmed to cope with the unexpected.

The role of stock index arbitrage is harder to assess....

...traders say that it may have begun a wave of selling that was then exaggerated by portfolio insurance programs.

In retrospect, the portfolio insurance programs may have helped create much of the turmoil that ultimately defeated them.

"The problem was that everyone is working from roughly the same theories," said Peter U. Vinella, a partner at Berkeley Investment Technologies in Berkeley, Calif., which writes many complex trading programs. "They all get the same feedbacks. And that leads everyone to take the same action."

A Fear of Defying the Computer

Why do people become captive to computers? Programs, of course can easily be overruled by humans, who make the final decision about whether to proceed with a transaction. But amid chaos, when seconds could mean the difference between profit and ruin, traders are deeply reluctant to disregard the neat columns of computer-generated instructions.

"People get lulled into thinking, `My program says this will work,'" said Robert H. Mundheim, the dean of the University of Pennsylvania law school.... "And you don't have time to think through the assumptions that went into the programs -- if you understood them in the first place."

[Discussion of whether a fully automated trading system might have avoided some of the panic that set in when orders were backed up for hours, causing investors to sell even more.]

Slowing of Market Studied

Investigators have already discarded as unenforceable one option: stopping the use of computer programs that speed the pace of decision-making. More practical, experts say, would be actions that slow the market, giving participants a chance to absorb new data and adjust accordingly....

Search RISKS using swish-e

Report problems with the web pages to the maintainer

Search RISKS using swish-e

THE RISKS DIGEST

Forum on Risks to the Public in Computers and Related Systems

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

Volume 5: Issue 82

Wednesday 23 December 1987

Contents

NYT article on computers in stock crash

P. T. Withington <PTW@DIAMOND.S4CC.Symbolics.COM>
Wed, 23 Dec 87 11:51 EST

An article in the Boston Globe yesterday (23 December) covers similar issues, but raises a few additional points which make me think that (as usual) the computer is only an unwitting accomplice and not the source of the trouble at all.

> Date: Mon, 21 Dec 87 21:48:36 EST
> From: hal@gvax.cs.cornell.edu (Hal Perkins)
> [...]
> Promotions [of portfolio insurance] worked: By October, between $70 billion and $90 billion was invested in funds using some form of the insurance....

The Globe article points out that when portfolio insurance was first "invented" it was dismissed in an article in Fortune (ca. 1980) as a "carnival act". Its inventors pursued its promotion however, and the "invention" of index futures allowed them to make the concept more palatable to fund managers (since they were no longer required to change the makeup of their portfolio to participate). Shortly to follow was the "invention" of index arbitrage, which provided a ready appetite for the portfolio insurers' future trading.

My inference is that what legitmized the "carnival act" was not any understanding of its mechanism, but simply a track record. Unfortunately there are a large number of investors who believe that history is an accurate predictor.

[...]

> "The problem was that everyone is working from roughly the same theories," said Peter U. Vinella, a partner at Berkeley Investment Technologies in Berkeley, Calif., which writes many complex trading programs. "They all get the same feedbacks. And that leads everyone to take the same action."

Here is the nub. My inference is that as long as insurance and arbitrage were *unusual* investment policies, they actually "worked" by trading on discrepancies arising from imperfect information. Of course their success led to popularity, and eventually to the situation Vinella describes: all sellers and no buyers, the downfall of any Ponzi scheme.

> A Fear of Defying the Computer

[...]

> "People get lulled into thinking, `My program says this will work,'" said Robert H. Mundheim, the dean of the University of Pennsylvania law school.... "And you don't have time to think through the assumptions that went into the programs -- if you understood them in the first place."

The Globe points out that the inventors and primary promoters of portfolio insurance (LOR Corp.) actually did "sanity check" what their computers told them to do and held off making the massive futures sales the program directed. (I believe they realized, if only intuitively, that their algorithm was operating out of its useful range, because they had not forseen the discrepancies it was now receiving as inputs.) However, several of their licensees did exactly as the program directed, having been lulled into beliving in its infallibility, only to find there were no buyers. As the sell orders mounted, depressing the price, the algorithms, lacking any sanity checks, simply directed more sales.

It's interesting to speculate whether the limited automation of the exchanges exacerbated the situation or acted as a governor to slow things down enough for conventional investors to react to the bargain-basement prices and finally put a floor under the madness.

...BAD PRACTICE to truncate anything without notice (Re: RISKS-5.79)

Doug Rudoff <wiley!doug@uunet.UU.NET>
23 Dec 87 19:12:49 GMT

About two years ago I was working on a project that required coding in PL/I. I had a problem with running out of memory while exectuting my code. After many hours of frustration I discovered the problem was that I had two procedures 'put_message' and 'put_page' (which called 'put_message') truncated to the same name. This was due to PL/I's truncation scheme of taking the FIRST four letters and the LAST three of a procedure. Thus, both procedures were identified as 'put_age' and I ended up running out of memory because of unintentional recursive procedure calls.

Doug RUDOFF TRW Inc, Redondo Beach, CA {cit-vax,trwrb,uunet}!wiley!doug
H: (213) 318-9218 W: (213) 812-2768 wiley!doug@csvax.caltech.edu

> [Recursively Call a spade a spade a spade ... but don't expect it to return. (If it weren't Christmas time, and it hadn't been pouring in LA, I probably would have refrained from annotating this message from RUDOFF THE RED{ONDO} KNOWS RAINGEAR.) Happy holidays to all. PGN]

The spread of viruses and news articles (Re: RISKS-5.80)

Allan Pratt <ucbcad!ames.UUCP!atari!apratt@ucbvax.Berkeley.EDU>
Wed, 23 Dec 87 12:01:59 pst

<>The prank seems to be benign, and therefore beneficial.

My contribution was relevant to the above passage: the fact that it was on the front page of a major metropolitan newspaper (The San Fransisco Examiner, Sunday 12/20/87) with a more or less in-depth article spread the implicit warning farther (sociologically) than the virus itself spread. (Granted, this metropolitan newspaper serves one of the most computer-literate parts of the country...)

Opinions expressed above do not necessarily -- Allan Pratt, Atari Corp.
reflect those of Atari Corp. or anyone else. ...ames!atari!apratt

> [I think the major point about Trojan horses, viruses, and similar problems is that they are relatively easy to perpetrate, but potentially devastating on many systems. The cases we have seen to date are all rather benign (except for denials of service) or localized in effect (PC graphics ARF-ARF!). The lesson is that these vulnerabilities exist. However, the rather benign cases suggest that deeper concern is warranted. PGN]

Common passwords list

<Mansur@DOCKMASTER.ARPA>
Wed, 23 Dec 87 11:59 EST

I am interested in making a list of the most common passwords chosen by users. I'd like to see if anyone knows of any studies that have been done (I vaguely recall hearing of at least one such study). We are writing a program to check for poor passwords on our systems. Please send replies to:
Doug Mansur -or- (Mansur@dockmaster.arpa)
L-308, Lawrence Livermore National Lab., P.O. Box 808, Livermore, CA 94550P

[At one time "Susan" was reputed to be the most popular American choice. I recall a British clipping citing dogs' names as popular passwords. However, since many prudent system managers now insist on randomly generated pronounceable passwords, your study might be dated. Furthermore, I hope no one is stupid enough to tell you what their password is. But past studies (e.g., Morris and Thompson, UNIX Password Security: A Case History, CACM 22 11 November 1979) have encrypted initials, dictionaries, etc., with great effect. If your system permits access to unencrypted passwords, your study might focus on that instead. PGN]

Re: IBM Christmas Virus (RISKS 5.80)

Skip Montanaro <steinmetz!montnaro@uunet.UU.NET>
Tue, 22 Dec 87 13:33:10 EST

Ross Patterson wrote (in RISKS 5.80):

>(5) Is the Internet similarly vulnerable ?

<>Not to this one. It plays on several things that the Internet doesn't have:
<>1) A large number of IBM VM/CMS systems. ...
<>2) A suitable file transfer system. FTP doesn't apply. ...
<>3) A good method of determining targets. The CMS NAMES and NETLOG files ...

The quasi-equivalent of this problem in UNIX systems (and most of the Internet, because of the large number of UNIX systems it contains) is the ubiquitous shar file, an ASCII packaging machanism used to transfer code and other ASCII files via mail and/or Usenet news transfer. The problem lies in the way users unpack shar files: they execute them. Needless to say, inspection of shar files before execution/extraction is highly recommended.

There's nothing to prevent me from writing a shar file that purports to be a Christmas card. Execution of it might display the card, check out the contents of various mail-related files, (like ~/.mailrc and ~/mbox) looking for likely candidates to send the shar file, then recursively send it.

In fact, the same scheme would work for most operating systems with a command language that could be executed from a file. UNIX systems are especially vulnerable, however, because of their large numbers.

Skip (montanaro@ge-crd.arpa, uunet!steinmetz!sprite!montanaro)

Cleaning PC's can be bad for your health...

John McMahon <fasteddy%sdcdcl.span@VLSI.JPL.NASA.GOV>
Wed, 23 Dec 87 07:40:53 PST

The following "SAFE-ALERT" form was distributed at Goddard Space Flight Center (NASA - Greenbelt, MD) about cleaning PC's. The date was 7/29/87, alert number X7-S-87-01.

"Recently an employee of this installation was cleaning his personal computer screen with a glass cleaner when the screen caught on fire.

The computer had been in use for some time and had built up a static charge. When the employee went to wipe off the glass cleaner with a tissue, his finger hit the screen. This action discharged the static charge causing a spark which ignited the alcohol in the window cleaner. A total of 8 personal computers were checked, with only 1 other catching on fire."

The installation mentioned above was the Naval Weapons Center in China Lake, CA.

The action taken was to inform the employees about what could happen, and ask them to use a non-flammable cleaner. If there was a need for a flammable cleaner, then employees were advised to discharge the computer before spraying.

John McMahon DFTNIC::FASTEDDY (Span) FASTEDDY@IAFBIT (Bitnet)

PIN verification security

<MAKELA_O%FINJYU.BITNET@CUNYVM.CUNY.EDU>
Wed, 23 Dec 87 15:53 O

A while back, I posted an article on ATM card security, promising to tell more as soon as I get the official security guide. Well, now I have the guide, and here are some findings, given somewhat verbatim since this document was distributed as "confidential":

In Finland, there are two methods of off-line verification of PIN's. Both are DES-based, so they can be considered pretty secure (unless there are hidden trapdoors in DES - has the analysis behind its design been made public yet ?)

The PIN verification is done by the "verification unit", which consists of a keypad for PIN entry, the magnetic stripe reader unit and the main electronics unit, which communicates with the local cash register unit. The document also specifies which "security modules" may be used in these verification units: Intel 8751H, Intel 8752H and AMD 9761H. Can someone who knows better tell what these units actually are ? DES-chips ?

The first method of PIN verification is the same that is used in VISA-cards internationally: the card number, the PVV-version number (off the card's magnetic stripe) and the PIN number the customer has entered from

the keypad are all munged through DES, using certain highly secret keys which are distributed by the banks. The resulting number is then compared with the PVV-number from the card's magnetic stripe, and if it is same, the given PIN was correct.

The second method used is local to Finland, I guess. In this, the card number is encrypted with several highly controlled keys, resulting in the actual PIN that the client should have given. There are very strict rules on key control, for example the master key is divided into three parts and given to three people who each load their part to the verification unit ala bank safe keys.

This document also specifies the encryptation that MUST be used for all message transmissions to/from the verification unit. This would seem to remove problems with faked messages etc.

The only problem that would seem to arise is key security - if the keys become widely known, there goes the security.

Generally, it would seem that this type of security is an overkill in practise. A local supermart is a good example: they are on-line to the bank so they can send payment transactions immediately to the bank computer, they use magnetic stripe readers to read credit card / bank card stripes, but they still use signatures for verification. The only reason I can think for this is that it's simpler for them. Hooray for minimizing of risks!

A note on ATM's swallowing cards up: my girlfriend lost her card to another bank's ATM a couple of days ago, since she couldn't remember the new card's PIN right. She didn't want them to send the card by mail, since it would take a few days, so she called the bank the next morning and told them to keep the card, she'll come and pick it up. Then she just went there during her lunch break, showed ID, and they gave her card back to her, since the card was not "wanted" or anything. Banks over here seem much more cooperative then the american ones I've been to.

A safe Christmas, Otto J. Makela, U of Jyvaskyla
Mail: Kauppakatu 1 B 18, SF-40100 Jyvaskyla, Finland Phone: +358 41 613 847
BBS: +358 41 211 562 (V.22bis/V.22/Bell 212A/V.21)
BitNet: MAKELA_OTTO_@FINJYU.bitnet

Social Insecurity

Roger Pick <rpick@ucqais.uc.edu>
23 Dec 87 11:45:22 EST (Wed)

I have been reading RISKS for a number of months and have noticed that the contributors seem to take it for granted that social security numbers cannot be required except in situations involving income.

I would like to know what the basis for this common knowledge is. Is it a statute? A court case? Can you give me a name or a citation so I can look it up in our local law library?

The reason I am looking for it is that my health insurance plan is demanding my children's social security numbers. I seek to keep their social security

numbers private whenever possible in order to reduce the problems they will encounter if a Big Brother society should come about. (I give mine out without a second thought -- it is already in so many places that I would have no privacy anyway.) To be able to cite legal chapter and verse would significantly strengthen my case; the insurers are presently intransigent.

Roger Alan Pick - QA & Information Systems Department, University of Cincinnati
VOICE: (513) 475-7166
UUCP: {decuac,psuvax1!gatech!mit-eddie,philabs!phri,pyramid}!uccba!ucqais!rpick
POST: QAIS - Lindner Hall, Univ. Cincinnati, Cincinnati, Ohio 45221-0130 USA

[This question is like the Yes Virginia, there is a Santa Claus letter in the International Herald Tribune. Discussion goes back to early RISKS. PGN
]

Search RISKS using swish-e

THE RISKS DIGEST

Forum on Risks to the Public in Computers and Related Systems

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

Volume 5: Issue 83

Thursday, 24 December 1987

Contents

Another article on the Christmas Virus [just in time for Xmas]

Mark Brader <msb@sq.com>
Wed, 23 Dec 87 18:28:31 EST

> [In the spirit of the season, I am including this now rather old-hat and somewhat ill-informed note for a few more background details. It is interesting perhaps more for what the press can do to an incident than for the incident itself. Happy holidays to all. RISKS will take some vacation -- unless something really startling happens. PGN]

I have been handed a clipping from the (Toronto) Globe and Mail's "Report on Business" section. I don't have the date, but Texaco Canada Inc. closed at $31, up $4.50, on the other side of the page.

The clipping is of the Quidnunc column by Bud Jorgenson.
My !'s in square brackets.

> Merry Christmas, Big Blue. The internal system of the world's biggest computer company was disrupted for almost 72 hours by an

electronic Christmas card. IBM's public relations department played down the seriousness of the incident, but according to our mole at IBM, "it crippled us".

The computer equivalent of a nuclear meltdown [!] began at a university in West Germany when someone tapped into [!] IBM's Prof (PRofessional OFfice) System with a graphics-laden Christmas message. Whether it was deliberate or a coding error was not clear [!], but the card quickly became a hit and was passed on to various routing systems.

As every computer buff knows, graphics use large bites of memory and this one gobbled up an ever expanding chunk of the Prof System as it multiplied its way through IBM offices. This was a week ago Friday, just before quitting time in Europe and during the first half of the workday on this side of the water.

When the system goes down, IBM simply cannot work because just about everything is dependent on the [!] computer, right down to daily diaries with meeting schedules. By early Monday, the system in Canada was partly restored so that employees could tap into the data base to read files.

But they couldn't use printers or communicate with other offices until the all-clear was sounded, which was after 10 am Eastern time. An IBM spokesman said the impact on operations varied from country to country.

Police work to track down the culprit was turned over to Bitnet and Earn, a pair of computer networks that link universities in North America and Europe. The list of suspects has been narrowed to two at the Technical University of Clausthal, a small town south of Hanover.

Forwarded by Mark Brader, SoftQuad Inc., Toronto, utzoo!sq!msb

---

Social Insecurity (Re: RISKS-5.82)

<willis@rand-unix.ARPA>
Thu, 24 Dec 87 09:12:05 PST

Let's talk about the SSN some more, even tho it's been done a lot. Originally the SSN was the number that identified one's account with the SSA; hence, it was like a bank account number. As we all know, the cards and literature from the SSA all specificically say: Not an identification number. In fact it was called the SSAN.

As the SSN spread throughout society, someone along the way observed that it could play the role of a personal identifier. I do not recall, may not even ever have known, the first such occurrence.

The best definitive treatment of the SSN and its role in society is

chapter 16 of the report of the Privacy Protection Study Commission: Personal Privacy in an Information Society, July 1977, USGPO. I wrote the original drafts of the chapter, and at the time, it was factually complete and accurate. It is of course now 10 years old.

Generally speaking, there are only a few situations in which one is obligated by law to give his SSN. Aside from the SSA business, it generally revolves around tax reporting and secondary aspects of same. Thus, financial transactions require the SSN but it's still really a tax matter because the IRS wants to track financial matters in its own interests.

At least one state has required by law that the SSN be the driver license number and it was upheld in court; I think it was Virginia. Another state tried but was shot down in court; it may have been Illinois. UCLA tried to use it as a student ID but backed off when threatened by a student in a court case.

The point is that most organizations that ask for it do not have a legal basis for requesting it. Rather, it's more like a condition of doing business with the organization. In that respect, it's like one's phone number or driver license, one or both of which are commonly asked for in California when making a bankcard purchase. On occasion, I have challenged such requests, usually successfully, but it's always a hassle because the clerks are only doing as told. The phone number is easy; give any one that comes to mind. That one has never backfired on me; I and a lot of other people give a business phone. After all why asdvertise a residential number that you pay to keep unlisted?

I have corresponded with MasterCard about this, but it can do nothing to control the merchants. They do not require it of the merchants, and it's not clear to me why the merchant's even want the supplementary data. I suppose they believe that the driver license number may lead to a good current address and that a phone number may be useful in a collection action. I frankly feel uneasy about a phone number, a DL number, and a bankcard number on one piece of paper being handled by people who are not trained or accustomed to dealing with sensitive personal information. The combination of numbers makes it all that much easier to masquerade.

Organizations try circuitous ways to get the SSN. For example, when one gets or renews a driver license in California, he finds a place for inserting the SSN but without explanation. The sheep among the population of course fill it in without asking although there is no statement on the form saying that it is required. The presence of the blank space for the SSN implies that it is a required data item. If one asks about it though (and clearly I have) he's told that "it's optional". How about that as a way to finesse people and get data that the state has no legal basis for requesting? It's clear why they want it; it makes it easier to correlate DMV data with that from insurance companies.

Anyway, the best you can do is to ask anyone: Under what legal authority do you request my SSN? If there's no answer or a poor answer, then you're in the confrontation business -- which maybe you can win by escalating it up the line to the top of the organization. It's not unheard of for the administrative or ADP types to make a policy decision to use the SSN

without the concurrence or knowledge of the top management. My usual line of argument is: "You have no legal basis for requesting my SSN and you have no need for it."

If there is no legal basis for requesting it, your choices are:

1. Do business with another company, or at least, threaten to.

2. Continue to confront and ignore the requests as long as you can. Sometimes ignoring the request will make it go away.

3. Give an incorrect SSN number to satisfy the request, but realize that in doing so, there could always be a backlash if there happens to be a legitimate use for it. This amounts to seeding the recordkeeping system with noisy data.

I think it's rather clear what's going on. The company you deal with has adopted the SSN as a convenient personal identifier. You might be able to force it to issue its own identifier. Sometimes an insurance company will contract with some outsider for record keeping support so the decision may have originated elsewhere.

In the end, it's a Catch-22 situation. nne doesn't always have competition to give him alternate choices, or he may prefer the company that's bugging him. All any of us can do is drag our feet, refuse as often as possible, and bring pressure wherever possible. At the same time we need to know when we're legally obligated to give the SSN and what the penalty is for not doing so.

That'a quick once-over lightly.

One individual at Los Alamos contested a request for his SSN and as I recall, with success. I don't wish to intrude on his privacy by publishing his name/contact publicly. If you're interested in his case, I'll pass along names/addresses to him.

Willis H. Ware, Rand Corporation

Expert systems (RISKS-5.78)

Peter da Silva <nuchat!sugar!peter@uunet.UU.NET>
24 Dec 87 01:00:54 GMT

Re: the folowing comment on the use of expert systems in environments where the system's decision making process can't be examined...

> For example, a pilot flying an aircraft through a fly-by-wire system can't examine all the control logic while flying the airplane. We can (and should) strive to give as much pertinent ...

Perhaps we should avoid using poorly understood systems in real-time applications. It's debatable whether expert systems would actually buy you any efficiency in this case, but even ceding this point efficiency is not

the only criterion in the design of control systems. Repeatability is at least as important.

-- Peter da Silva `-_-' ...!hoptoad!academ!uhnix1!sugar!peter
-- Disclaimer: These U aren't mere opinions... these are *values*.

[Between Peter G. N. and Peter da S., this topic has been a real Repeter. But these sentiments are clearly a concern of the RISKS Forum. PGN]

Most-common passwords (RISKS-5.82)

Rodney Hoffman <Hoffman.es@Xerox.COM>
24 Dec 87 12:15:00 PST (Thursday)

In Security Interest Group Digest of 12 Nov 86, Bob Baldwin <baldwin@xx.lcs.mit.edu> posted a list of likely passwords arranged by category. Though it doesn't say so, I believe the list is from college student accounts. The common categories were:

Obscene words
Favorite music (group names, albums)
Ego strokes (lord, wizard, ...)
Cartoon names and places
Car names
Insults to computer (farce, slave, ...)
Female names
Male names
Funny words (whynot, foobar, simple, ...)
Spy terms (secret, password, ...)
Keyboard sequences (qweasd, poiqwe, ...)
Tolkien characters and places
Popular fiction and sci fi (characters, titles) esp. serials
Doubled 3 letter groups (sexsex, foofoo, ... esp. user names doubled).
Pet names (bowser, ...)
Reversals (terces, drawkcab, ...)
Composers
Passwords for dead accounts (deadacct, unused, ...)
Passwords based on host name for people with lots of passwords
(e.g., for a system is named "cls": clspass, clspwd, ...)

Permissions and setuid on UNIX (Re: RISKS digest 5.57)

Philip Kos <decvax!osiris!phil@ucbvax.Berkeley.EDU>
Fri, 20 Nov 87 11:58:41 EST

I thought a reply to David's exhaustive explanation of the "correct" use of UNIX setuid to allow copying otherwise unreadable info (RISKS 5.57) was warranted. His description of setting up special groups to make the student's file readable by the setuid-teacher process is interesting, but as unnecessary as it is (admittedly) ungainly.

> From: oster%dewey.soe.Berkeley.EDU@Berkeley.EDU (David Phillip Oster)
> Subject: UNIX setuid stupidity
> Date: 6 Nov 87 20:08:36 GMT
> ... [the task] would copy a file owned by a student into a directory
> owned by a teacher. ...

The method David described will certainly work but is unnecessarily complicated. What is really needed is for the copy process to use its effective uid (teacher) to open the target file, and then use its real uid (student) to read the source file.

open() uses the effective uid (not the real uid) which makes it possible to open the teacher's file, but not to open the students's file. However, the proper permission is needed only for the open(), and not for any read()s or write()s. This makes it possible to create the teacher's file *and* open the student's file for reading within the same process, by fiddling with the process' effective uid.

(Aside: I recently debugged a problem with another local setuid process which was using the access() system call to determine whether or not a data file should be written. I have to wonder about the usefulness of access(), which uses the process' real uid to check permissions, when the real uid is virtually useless because of open()'s use of the (different) effective uid for the same purpose.)

The scheme is to open() the teacher's file, then set effective uid to real uid, then open() the student's file and perform the copy. The basic copying procedure thus becomes more complicated, but any global mucking around with the system (like dynamically creating and removing a unique group id, or statically assigning unique group ids for each (teacher, student) pair at the beginning of a school term) is avoided.

A simple implementation using /bin/cat to do the actual copying follows. This code works on a Pyramid running OSx version 4.0 (OSx is a "dual port" 4.2BSD and SysV.2 UNIces); it should work on any "real" UNIX system, using either setuid(getuid()) (as shown) or the appropriate combination of getreuid() and setreuid(). Extension to handle multiple files should be simple enough if it is necessary.

...!decvax!decuac!\ Phil Kos
...!uunet!mimsy!aplcen!osiris!phil The Johns Hopkins Hospital
...!allegra!/ Baltimore, MD

[PLEASE CONTACT PHILIP DIRECTLY IF YOU WISH THE PROGRAM... PGN]

UNIX chroot and setuid (Re: RISKS-5.71)

Michael S. Fischbein <msf@ames-nas.arpa>
Tue, 8 Dec 87 05:50:37 PST

I must disagree with the conclusions drawn by the comment in RISKS 5.71 that chroot() will not prevent a setuid program from accessing the rest

of the system. The scenario described will allow such access BUT proper design of a setuid() program designed for security will prevent this.

The foundation of any classified data system is the `need to know.' Analogously, the foundation of a security conscious computer program must be that only sufficient permissions to do the required task are granted. If you only need to read the data in a file, you do not get write permission. For setuid()/chroot() programs, the user whose ID is being set to should NOT EVER be root. ROOT SETUID SHOULD ONLY BE USED IF ACTUAL ROOT PERMISSIONS ARE REQUIRED. If you are setting up a chroot() section of the tree, all required permissions could easily be satisfied by having a dummy user number to own all the system files, directories, etc in that section of the tree. Full protection could involve rewriting the system calls for open() to not allow root type access to programs linked with the system library in the restricted part of the tree. This step is not necessary; setuid() is a powerful tool that is easily toned down to the appropriate level by selecting an appropriate user id to set to. Don't use root unless it is necessary.

In fact, the setuid() call itself is overused. Most programs that require the sort of permissions revisions that setuid() permits can get by with setgid().

mike
Michael Fischbein msf@prandtl.nas.nasa.gov ...!seismo!decuac!csmunix!icase!msf
These are my opinions and not necessarily official views of any organization.

[These last two messages have been backlogged for a while. I think they are of interest. However, it is important to note that there are many other vulnerabilities as well, and attempts to patch around or use carefully a particular vulnerability does not imply the absence of other problems. So please temper any future contributions accordingly. PGN]

Search RISKS using swish-e

THE RISKS DIGEST

Forum on Risks to the Public in Computers and Related Systems

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

Volume 5: Issue 84

Thursday, 31 December 1987

Contents

Risks of Robots (From comp.sys.apple)

hpfcrs!eye!erich@hplabs.HP.COM <Eric Haines>
Wed, 30 Dec 87 09:44:31 mst

Reach for the Sky.

The US Department of Agriculture has encountered an unanticipated difficulty in its project to develop robot fruit pickers. To contain costs, the robots were designed with monochrome scanners. Unfortunately, to the robots, an orange has

the same size, shape, and brightness as a small cloud. Current robot pickers are often hung up literally reaching for the clouds. The USDA says it's back to the drawing board - this time using color.

(From "Random Access", 21 November 1987)

[Was this in Orange Count-y? By the way, a cotton-picking robot might still have trouble with white clouds. Fruit-of-the-zoom? PGN]

Christmas Exec AGAIN!

Eric Skinner <ERS2F%UOTTAWA.BITNET@CUNYVM.CUNY.EDU>
Wed, 30 Dec 87 11:31:51 EST

An interesting point that has not been mentioned so far is that, at least in the version that reached BITNET sites in Canada, there was a major bug in the code of the program. It parsed the NAMES file in a very inflexible way causing it to have a success rate of about 5% at coming up with valid forwarding addresses.

If the programmer had been more careful, we might have been in an even bigger mess.

So there are fewer risks when a program has bugs? :-)

Eric Skinner, Computing Centre, University of Ottawa

Computer glitch stalls 3 million bank transactions for a day

<Hoffman.es@Xerox.COM>
25 Dec 87 15:54:56 PST (Friday)

The Dec. 24 Los Angeles Times reports that "an unexplained computer glitch caused a one-day delay in posting an estimated $2 billion in transactions at First Interstate Bank of California last week." The data processing problem affected all checking account transactions last Thursday -- 3 to 4 million, both deposits and checks, an estimated $2 billion total.

For unexplained reasons, the entire record of Thursday's transactions from the bank's branches was rejected by the computer when posting was attempted at 10:30 pm Thursday. DP employees worked on the problem all night and the following day, and the transactions were finally posted late Friday afternoon.

The problem was corrected in time to avoid any widespread effect on customer accounts. A bank executive VP said, "We did not have a disaster. We had a systems problem that we are still diagnosing to make sure it doesn't happen again."

Switch malfunction disrupts phone service

Richard Nichols <ihnp4!chinet!rdn@ucbvax.Berkeley.EDU>
29 Dec 87 12:03:31 CST (Tue)

Copied without permission from the Post Tribune (Gary , IN)

MALFUNCTION DISRUPTS GARY PHONE SERVICE FOR 18,000 CUSTOMERS

GARY -- Many people living or working here found it impossible to use the phone early Thursday [Dec. 10, 1987]. A malfunction during routine testing of equipment at an Indiana Bell Telephone Co. switching office at 725 Madison St. was blamed by telephone company officials for disrupted service for abount 18,000 customers with 881, 882, 883, 885 and 886 prefixes. Gary police and fire department representatives said the city's 911 line was working, so emergency vehicles were able to respond to calls. Non-emergency business lines were out of service, they said.

The equipment failure occured at 5:45 a.m. with some phone customers regaining partial service by 7 a.m., said Estel Gibson, media relations manager for Indiana Bell in Indianapolis. Service was restored by afternoon, he said. Gibson said that during the testing, equipment was switched to battery power. The battery power was low and there was no warning, so when equipment was switched back to commercial power, the computer memory system was knocked out, requiring reprogramming of the computer, he added.

Besides five Gary phone prefixes, the system malfunction also affected access to long distance lines in north Lake County, said Gibson. Local calls were not affected outside Gary, he added. Gibson said the malfunction in switching equipment affected 18,400 lines in Gary. "Our first priority was to restore service," said Gibson. The second priority was to check the backup system to make sure it is working properly, he added.

At Methodist Hospital Northlake Campus in Gary, the nursing coordinator had to use a two-way radio for communications inside the building, a hospital representative said. At St. Mary Medical Center in Gary, calls were routed through the switchboard at the Gary hospital, a hospital representative said.

40,000 telephones on "hold"

Bob Cunningham <bob@loihi.hig.hawaii.edu>
Tue, 29 Dec 87 10:08:59-1000

Almost 40,000 Honolulu telephones were in and out of service yesterday (the first working day after Christmas), including the police/fire emergency number 911, and non-emergency Fire and Police numbers, due to a possibly faulty computerized switch, and an unusually heavy volume of calls.

The 40,000 customers were in 8 Honolulu exchanges, covering a large section of the downtown area. Unlike the 5,000 or so phones that were down during last the heavy rainstorm last week, this problem was not weather-related.

John Harper, Hawaiian Telephone's Director of Public Affairs explained that when the volume of calls rises to a high level, rather than falter completely the switching equipment goes into a "half load" status, handling only some incoming calls and often not delivering a dial tone to customers within the affected exchanges. The unusal aspect of yesterday's problem was that the volume of calls was nowhere near its rated load capacity. However, the switch was also busy doing extensive automatic self-diagnostics in order to locate an internal malfunction that it had detected within itself.

Hideto Kono, the chairman of the state Public Utilities Commission---whose phone was one of those affected---was very upset, saying that the recent outages caused by flooded cables were "understandable and excusable," but yesterday's problems were not. "Equipment is available that works well almost all the time, and we're going to be asking Hawaiian Telephone why its present equipment can't operate that way."

Bob Cunningham, Hawaii Institute of Geophysics, University of Hawaii

---

Unions denied access to commercial database services

John Saponara <saponara@tcgould.TN.CORNELL.EDU>
Thu, 31 Dec 87 10:41:15 EST

Eric Haines

>From: mt@MEDIA-LAB.MEDIA.MIT.EDU (Michael Travers)
Subject: Unions denied access to commercial database services

I came across this in InfoWorld (Nov 23, 1987). It has some scary implications about the desire and ability of corporations to control access to information. This points up the need for alternative power structure databases such as those that were discussed on prog-d a few months ago.

- - - - - - - - - - - - - - - - -

Restricted Access Riles Dialog Users
by Jeff Angus and Alice LaPlante

Subscribers to on-line databases may increasingly see the words "unauthorized file" when they try to use certain services, if a recent trend continues unchecked.

Last week, Dialog Information Services, a carrier of Dun & Bradstreet financial databases--including the now-restricted Dun's Financial Records--told labor union librarians that they would no longer be able to access certain files.

"If it's allowed to go on, this could set a precedent for a wide range of discrimination in online services, which are essentially public utilities," said Randy Barber, a financial consultant with the Center

for Economic Organizing, in Washington.

This time the discrimination is aimed specifically at labor unions and possibly the IRS, according to Barber. But if online services such as Dialog can cut off certain subscribers simply because of fears about how the data will be used, the next step could be routinely forbidding customers to access certain files at the slightest hint of an adversarial motive, according to Barber.

"It could get to the point where you'd have to have a demonstrably benign reason to access certain data," said Barber. "This precedent could have severe repercussions on the free market for ideas."

According to the AFL-CIO's librarian, Ruby Tyson, when she first got the "unauthorized file" message while trying to access the Dun database, she was referred by Dialog to the New Jersey office of Dun & Bradstreet On-line Services, where a spokesman told her a list of 240 "entities" had been compiled and sent to Dialog with the instructions to deny access to any person or organization on that list.

"We were told it wasn't just unions but other groups, including the IRS," Tyson said, adding that Dun & Bradstreet hinted the ban might be extended to other databases as well.

Both Dialog Information Services and Dun & Bradstreet refused to comment, but Marvin Hrubes, an attorney representing the United Food and Commercial Workers International Union (UFCW), sent a letter to both organizations charging that Dun & Bradstreet's actions constitute tortuous interference with the UFCW's contract with Dialog and are violations of the National Labor Relations Act and the civil rights laws of both California and the District of Columbia.

Tyson as well as Ellen Newton, librarina of the United Food & Commercial Workers International, say Dun's on-line information can be gathered through hard copies of the data. But this defeats the purpose of subscribing to an on-line service since researching and tabulating data manually using hard copy is complex and time-consuming, they said.

Tyson and Newton find the Dun move and Dialog's assent to it not only an inconvenience, because the service is so productive, but also an offense to their librarians' sense of the appropriate access to information, they added.

"We think it's a serious matter and something that causes concern for libraries in their role of providing access to the broadest possible diversity of ideas," said Patrice McDermott, the assistant director of the Office for Intellectual Freedom of the American Library Association.

Newton added that he has seen the information spreading. "Dun & Bradstreet has also knocked us off of Data Times," he said. "We just got a message saying that Dun's database service is unavailable under our agreement, which can't be true because we haven't signed any new agreement since Data Times added the Dun Service."

Newton spoke to a Data Times spokesoman who said that Dun & Bradstreet had

also sent his company a list of names of entities to be denied access.

'Leg Irons' Keep Inmates Home

Randy Schulz <bilbo.randy@SEAS.UCLA.EDU>
Sun, 27 Dec 87 14:05:34 PST

The following article, whose headline is the Subject: line of this message, is from the "Fourth District Report" (a newsletter sent to all constituents) issued by Los Angeles County Supervisor Deane Dana's office, dated Winter 1987-88. Carefully quoted verbatim (mistakes and all) and in its entirety w/o permission. No copyright notice appears on the newsletter:

> A modern-day version of "leg irons" is now being used to monitor the location of selected Los Angeles County inmates who as a term of their sentences are generally restricted to their homes.
>
> It is part of a pilot program that extends through September, 1988, using Comptom area probationers selected by the courts. The electronic devices are attached to the probationers' legs. Their movements are monitored by Trax Monitoring, Inc., which provided the devices.
>
> When we are faced with a jail overcrowding problem of tremendous proportions, elecronic surveillance of those probationers deemed suitable for the program offers at least a partial answer."
>
> At present, county jails have some 20,000 prisioners detained in facilities designed for 12,000 inmaates.

Paragraph three is apparently a quote, probably from supervisor Dana, though it is missing an open quote mark and an attribution, as you can see.

Although no real information on how the system manufactured by Trax Monitoring, Inc. operates, it is probably reasonable to assume that computers are a part of it. That there may be risks to the public in its use seems a fair bet.

While it's clear that this system is being used experimentally only on low-risk "inmates", there is presumably an interest in expanding its use as a "cost-effective" alternative to prison/jail construction.

In the same newsletter there is an article entitled "DRUGS. Experts map 32-point plan". Here are some excerpts from that article:

> Education, automation and methods to improve interagency communcation are the focal points of a 32-point list of recommendations by the Los Angesles County Task Force on Drug Abuse to stregthen the public's war on drugs.
>
> ...Other recommendations include:
>
> Increased automation on probation conditions; establishing a centralized repository of data on drug arrests, seizures and trends to be available countywide; standardized certification for drug diversion programs for

length, content, defendant participation and random drug testing; and,
regular meetings among representatives of drug enforcement, abuse services
and prevention-education agencies to discuss and resolve problems.

[Please pardon the poor grammar of the staff of my County's elected
officials...]

Randall Schulz, Locus Computing Corporation, 213/452-2435
{trwspp,ucivax}!ucla-va!ucla-cs!lcc!randy
{ihnp4,randvax,sdcrdcf,ucbvax,trwspp}!ucla-cs!lcc!randy

Re: Logic Bomb case thrown out of court (RISKS DIGEST 5.80)

Amos Shapir <nsc!taux01!taux01.UUCP!amos@Sun.COM>
25 Dec 87 14:20:53 GMT

In article <12360370542.28.NEUMANN@KL.SRI.COM> Geoff Lane writes:
>There used to be a problem in British law (and it may still exist) in that
>evidence could only be given by humans. Information generated by a computer
>without the explicit involvement of a human could not be used in court.

They do have a case here - anyone who has supervisor permissions on almost any computer system (and these might be obtained illegally) may generate any information, including hiding the traces of what s/he had done. After all, it's all just bits! So almost nothing can be proven without a reasonable doubt.

The problem is, this also applies to digital recording - both audio and video. A person with the right (wrong?) equipment can generate a video clip showing anyone committing any crime!

Amos Shapir (My other cpu is a NS32532)
National Semiconductor (Israel)
6 Maskit st. P.O.B. 3007, Herzlia 46104, Israel Tel. +972 52 522261
amos%taux01@nsc.com (used to be amos%nsta@nsc.com) 34 48 E / 32 10 N

Missouri Court Decision on Computerized Voting

Charles Youman (youman@mitre.arpa) <m14817@mitre.arpa>
Tue, 29 Dec 87 09:17:53 EST

While I was in St. Louis visiting my inlaws over the holidays, I read an article in the local paper about a court decision that found the computerized voting process used in Missouri was discriminatory. The loser of a close election had filed the suit in question. I didn't save the article and I don't think the article explained what was discriminatory about the voting procedure. The article did say that similar procedures were used in other states.

Charles Youman (youman@mitre.arpa)

<*minow%thundr.DEC@decwrl.dec.com*>

(Martin Minow THUNDR::MINOW ML3-5/U26 223-9922)
Date: 25 Dec 87 12:15
To: risks@kl.sri.com
Subject: pc hard disk risks

The discussion about virus programs reminds me that one thing I wish my PC's hard disk had was a "write-enable" switch, so I could test new programs with less worry about system corruption. (Also, the disk manufacturers and/or pc vendors don't seem to distribute anything resembling test software).

Martin Minow minow%thundr.dec@decwrl.dec.com

Viruses and Goedel bugs

<weemba%garnet.Berkeley.EDU@violet.berkeley.edu>
Sat, 26 Dec 87 02:43:06 pst

Last spring or summer the journal _Computer Security_ (?) carried a paper about the author's (company approved) experimentation with viruses. Alas, his research was closed down by his company, who got extremely nervous. Sorry I can't be more definitive; I'm surprised no one has mentioned this paper before.

The self-referential photocopier duplexor error that prevented the user from finding out what a duplexor was forms the key point of the plot of the fabulous science fiction story "Ms Fnd in a Lbry" by Hal Draper. (It's in Groff Conklin's _17 x Infinity_, beyond that I don't know.) (TOTAL SPOILER FOLLOWS...) Information is compactified into "nudged quanta", so the total primary knowledge of the galaxy fits in a single drawer. However, the secondary and higher order knowledge to >find< the primary knowledge grew exponentially. At some point, a certain nth-order quanta got stuck; checking for repair information got routed through that very quanta; emergency checking for the location of that original drawer of primary knowledge .... And so civilization collapsed instanter.

(Also, the bug reminds me of the true Cray story I submitted anonymously long ago, where an array bounds overflow corrupted the Fortran formats that attempted to trace the array.)
-Matthew
ucbvax!garnet!weemba Matthew P Wiener/Brahms Gang/Berkeley CA 94720
