RISKS TO THE PUBLIC IN COMPUTERS AND RELATED SYSTEMS

Peter G. Neumann [*SEN* Editor and Chairman of the ACM Committee on Computers and Public Policy], plus contributors as indicated. Opinions expressed are individual rather than organizational, and all the usual disclaimers apply.

Computerized public records boon to private eyes probing suitors (From Jay Elinsky)

From "Boy Meets Girl, '89, Can Be a Detective Story", Dirk Johnson, the New York Times, 10-Dec-89, p.1:

''Computerizing of public records in recent years has proved a boon to investigators, who say they can find out almost anything simply by keying a Social Security number into a computer... 'It's usually very easy', said Ed Pankau, the president of Inter-Tect [a Houston investigative agency], who is the author of 'How to Investigate by Computer'.'' ... ''Eager to trust but determined to verify, many single women in this age of risky romance are hiring private detectives to check the backgrounds of their suitors.'' ... ''Women are far more likely than men to hire an investigator, and usually their suspicions are on the mark, detectives said.''

In this case I'm tempted to call easy access to records (assuming it's legal) a benefit instead of a risk. Then again, I got married ten years ago, and my fiancee's investigation of my background was more traditional, like meeting my parents and using her "feminine intuition". And the article ends with a non-computer-related risk: The woman who is the subject of the article had three men investigated and found "skeletons in their closets". The fourth man she investigated was a-ok, and she was so thrilled that she told him he had passed the investigation. He wasn't thrilled to hear that he had been investigated. "'He kind of freaked out', she said. 'But then, as I tried to explain why I did it, he understood, kind of'. She added, 'We're not dating anymore.'" [Jay Elinsky]

(From Jon von Zelowitz)

[...] For $500, the Inter-Tect investigative agency in Houston promises to verify within a week a person's age, ownership of businesses, history of bankruptcies, if there are tax liens, appearance in newspaper articles, as well as divorces and children. Some clients have paid the detective agency as much as $10,000 to unearth secrets. ''People want to find a quality partner,'' said Mr. Pankau, who is a former investigator for the Internal Revenue Service. ''I wouldn't say they're paranoid, but they're very cynical.''

Re: private eyes probing suitors -- Amazon Women on the Moon (From Dwight D. McKay)

There's an amusing but scary skit in the movie, "Amazon Women on the Moon" regarding a women who checks out her boyfriend.

On a blind date, he arrives at her place. She asks for his driver's license and a valid credit card. She walks over to her desk and runs the credit card through a magnetic strip reader (like at a store) and gets a printout of all the other dates he's had and how they turned out...

Computer multiplies taxable earnings by 100 (From Rodney Hoffman)

Hundreds of independent employees who worked for Wells Fargo Co. two years ago were stunned to learn of a computer error that multiplied their earnings by 100 before passing on the information to the Internal Revenue Service. The IRS, eager to collect Uncle Sam's share, has written to the taxpayers, demanding an explanation for the discrepancies between the Wells Fargo reports and the recipients' 1987 tax returns. "I was panicked. They moved the decimal point two places to the right," real estate appraiser Harold M. Samuelson told the Salinas Californian. ['Los Angeles Times' 2-Oct-89]

Bug in Intel 486 chip

Compaq discovered a flaw in the trigonometric functions in testing the new Intel 486 chip. (Chips without the flaw were subsequently made available.) The chip contains 1.2 million transistor equivalents, and at 12 to 15 MIPS is three times faster than the 386 chip. 200 companies are reportedly actively designing new computers using the chip, and some were affected by the delay. [San Francisco Chronicle, 27 Oct 1989. See also *Computer Design* (News Edition) 28(2), 13 Nov 1989, p. 1.]

[Are these the chippies who can talk about a better MOS TRAP for which everyone makes a beaten path to their door?]

Faults in 29000 RISC chip (From Jon Jacky)

"Stepping on 29000 Bugs", Michael Slater, *ESD: The Electronic System Design Magazine*, Nov. 1989, p.22

The current stepping of Advanced Micro Devices 32-bit RISC processor, the 29000 revision D, still has three acknowledged bugs. However, the bugs are all relatively minor. They consist of an instruction burst mode problem, an exception handling priority error, and a data-access exception problem.

Since hardware workarounds have been required for the instruction burst mode problem since the first silicon, existing designs either already incorporate the fixes or don't produce the offending set of conditions. Modifications to the exception handlers can correct the other two bugs. These same bugs were also present in revision CA. The most serious bug from revision C, the failure of the branch target cache to work reliably, has been fixed. ... AMD has distributed samples of the new revision, and current orders are expected to be filled with this revision.

Computer misdirects phone calls for TV programme (From Olivier Crepin-Leblond)

"Yorkshire cricket fans were hit for six [that's six runs... - OCL] when they were invited to take part in a Yorkshire TV phone-in and received sex advice instead. After a programme called 'What's to do about Yorkshire Cricket', viewers were invited to ring a special number to give their opinions. But when they dialled, they heard a recorded message from 'Barbara' about sexual problems. British Telecom (BT) blamed a computer fault... " [ORACLE Teletext TV News Service, 16 Nov 89] [I presume 'Barbara' was not blaming computers for anyone's sexual problems. PGN]

Coping with the unexpected - another stock plunge (From Steve Bellovin)

The AP wire service provides financial page tables for many newspapers. As part of the process, they filter out trades that are more than 3% off of the current price. That didn't work on Friday the 13th of October 1989, when the market plunged; they were forced to adjust their filters to accept 50% differences. The data was manually filtered before the weekend editions to eliminate trades that were ''clearly reported incorrectly''.

Quotron gores the bears and bares the bulls. Oxidentally. (From David B. Benson)

''Traders ... were stunned to see the Dow Jones Industrial Average plummet 99 points in seconds. A minute later it soared 128 points, then zoomed back down 113 points, 69 below Friday's close. ... Quotron Systems Inc., a Citicorp unit, blamed the 30-minute foul-up on "a timing problem in our software" caused by the enormous early volume -- about 145 million shares in the first hour of New York Stock Exchange trading. The prices of the individual stocks that make up the average were correct, Quotron said, but the average was wrong. ... It was the second time in less than a week that Quotron has had problems calculating the industrial average. ... [The earlier problem was attributed in a previous article to human error.] A Quotron spokeswoman said recent software changes may have contributed to yesterday's problems. She said Quotron switched to a backup system until the problems were corrected.'' ['Traders Who Can't Believe Their Eyes Win Vindication, Heavy Stock Volume Makes Some of Quotron's Data Veer Away From Reality', by Georgette Jasen, The Wall Street Journal, October 17, 1989, page c23]

UK Banking Error (From Brian Randell)

[I have used the hash symbol (#) for the pounds symbol. I am assuming that the the story is using the term "billion" with its normal American meaning! BR]

Bank Error Hands Out #2bn in Half an Hour
Computer Weekly, Thursday 19 October 1989, p.1, by Tony Collins,

A UK bank has accidentally transferred #2bn to UK and US companies because a software design flaw allowed payment instructions to be duplicated. The organisation has asked customers to return the money, which is more than the annual profits of any clearing bank, but so far not all of the cash has been recovered. The error, described by the Computing Services Association (CSA) as probably the most serious to have hit the IT industry, led to the #2bn being paid out to customers over 30 minutes.

Within an hour the bank discovered its mistake, but by then the cash had been transferred to other banks and into accounts of corporate customers in the UK and US. The funds were sent on the high-speed Clearing House Automated Payment System (CHAPS) which allows high value payments, typically #2m, to be transferred in seconds from one bank to another via a computer system linked through British Telecom's Packet Switched Service.

Although CHAPS refuses to name the bank it confirms that the accidental transferral of #2bn occurred "in the past few weeks" and involved one of its 14 member banks. The membership includes all major clearing banks together with the

Bank of England, Girobank and the TSB. Jim Reeves, CHAPS technical manager, says funds transferred on the network are guaranteed payments and are technically irretrievable. "If a bank decides it has made a mistake, it is still bound to settle the funds at the end of the day." He adds that, as far as he knows, most of the #2bn has been recovered as a result of the goodwill of the close-knit banking community and its corporate customers. "One bank managed to send a number of payments it had sent the day before," says Reeves. "It only noticed this because of a very high outflow of money early in the day. It was a question of getting in touch with customers and asking them if they minded payment going back."

Richard Allen, chief executive of the Association for Payment Clearing Services (Apacs), which controls CHAPS, says security and reliability have become increasingly important in payment mechanisms, especially as more institutions began using such systems. "This is particularly so in high value mechanisms such as CHAPS," he says. Reeves says the #2bn involved mostly foreign exchange and money market transactions. The error was due to a software flaw which allowed the system to choose a date for payments rather than insisting that the operator made the selection. In the event the system chose the wrong date. The software has since been redesigned to avoid a repetition of the incident.

There was follow-up article in Computer Weekly (Oct 26, 1989, p.9). The nicest bit in the new article is where it indicates that the story was originally broken in a speech by Jim Reeves, technical manager of the Clearing House Payment Systems (CHAPS) to a gathering of bankers and other financial industry delegates at the Compsec computer security conference: "Reeves struck observers as the most unlikely bean-spiller in the financial industry. His voice was so unexpressive that his Compsec speech left one immaculately dressed banker in the audience slumped across two seats, snoring loudly. The enormity of the #2bn error was lost on his audience. Yet Reeves was saying, in effect, that in a matter of minutes a systems or operator error could cost a bank more than its annual profits. ...

"Citibank insisted that there had been no financial loss to the bank or any third party as a result of the error. But this comment begs many questions which Citibank would not answer. What about the lost interest on the #2bn? Even a day's lost interest would amount to more than #500,000. ... To most people the idea that systems could be so vulnerable as to allow a criminal, perhaps organised criminals, to divert electronically hundreds of millions into false accounts would be inconceivable - just as incredible as the notion that a bank could pay out #2bn by mistake."

Coral reef ruined by poor user interface design? (From Jim Helman)

The captain of a ship that ran aground on an environmentally sensitive live coral reef off the US coast attributed the accident to a confused officer and a bad user interface. Apparently, an officer incorrectly changed course because the steering mechanism on the ship operated in the opposite fashion from most such controls. Whether or not the control was computerized, this demonstrates quite dramatically the potential dangers of inconsistent user interfaces. I suppose the company which built the control could be held liable for the poor design.

What if a company has to use an inconsistent interface because of patent restrictions? Could the company still be liable for the errors of a confused user?

[From a UPI article:]

"I think he made an error. I think he was confused," Capt. Zdravko Beran told Coast Guard investigators on the first day of testimony before a board of inquiry. "He told me that (navigational) light was dead ahead and then he wanted to turn a few degrees to the port (left)." Instead, the officer, Zvonko Baric, turned the ship to the right, or starboard, causing it to run aground on sensitive coral in the Fort Jefferson National Monument, Beran said. The steering mechanism must be turned in the opposite direction of the intended course -- the reverse of how most such devices operate, Beran said. Asked how future such accidents could be avoided, Beran said the federal officials could require ships to go around rather than through the national monument.

Computerized translation strikes again (From Joe Morris)

[From page R6 of the *Wall Street Journal*, Friday, 22 September 1989 comes yet another story of the perils of computerized translation of natural languages. The text below appeared in a sidebar to a story about the problems encountered in trying to resolve differences between European countries preparing for the 1992 amalgamation into the EC...]

Towering Babble -- Automatic translation system proves that to err isn't just human

Interpretation and translation gobble up a huge hunk of EC's central budget, so the Eurocrats have been trying to save money by using an automatic translation system. Systran is its name. Bloopers are its game.

To the unconcealed delight of those whose jobs it first appeared to threaten, Systran, acquired from the U.S. Navy about

10 years ago, still has a bit to learn about French-English translation. A few howlers:

• Commission President Jacques Delors asked in French whether he could address a certain committee. Systran had him asking whether he could 'expose himself to the committee.'

• Crown Prince Jean of Luxembourg, invited to offer a royal page of prose to the computer, used the words *nous avions*, which in context only meant 'we had'. Systran made it 'us airplanes'.

• In one screed about farming, the writer used the phrase *les agriculteurs vis a vis de la politique agricole commune*, which means 'farmers, in the light of common agricultural policy...' Systran, suffering either a blown microprocessor or an uncanny flash of insight, rendered it as 'farmers live to screw the common agricultural policy.'

[The article goes on for another nine column inches discussing non-computer related problems of translation, which are significant. In the headquarters of the Council of Ministers there are about 2000 bureaucrats, half of whom are translators.]

Risks of computerized typesetting: Angel Station Typos (Tor Books press release, from Chuq Von Rospach via Saul Jaffe as SF-LOVERS moderator, via Alayne McGregor)

Not too long ago, Tor SF author Walter Jon Williams got a very pleasant surprise: His science fiction novel 'Hardwired' (Tor, 1986) was prominently featured in a national advertising campaign for Nissan Motors' new "Infiniti" automobile. Apparently the Powers that Be decided that some law of good fortune had been violated. When Williams returned from the World Science Fiction Convention in Boston to linger over the pages of his newest Tor hardcover ANGEL STATION, he got a most un-pleasant shock: Not only was there a rash of very strange typographical errors on page 9 of the book, but fully seventeen lines of type were completely missing from page 354.

When Williams called Tor's editorial staff in New York to report the errors, they immediately checked the press run of the book. Sure enough, the defects were present in every copy -- despite the fact that all previous proof sheets, and the book's bound uncorrected galleys, were free of the errors.

This isn't "business as usual" for Tor. Although an occasional typo slips by the proofreading process, and minor errors creep into final copies, nothing of this sort has ever happened to a Tor book before. How did it happen? Well, no one knows exactly -- but the evidence points to some sort of software error in the generation of the final "repro proof" long after the stages at which books are normally checked and proofread in house. For example, the typos on page 9 all involve characters that are exactly five letters off in sequence from the correct characters.

Risks of Mail (From Joe Dellinger)

Several computers in the Earth Science department at Stanford were brought to their knees 13 Dec 89 by an interesting combination of bugs. I can only assume similar numbers of machines around campus in other departments also succumbed. I don't really know, because our network is dead as a result of it! For some reason, the Stanford Chinese Student association mailing list started bouncing mail infinitely between two Stanford machines, "Macbeth" and "Portia". At each iteration the 30K of mail was rebroadcast anew to everyone on the list, including at least one Chinese student on each machine in our department. This was the first bug. I don't know why it happened. (Anyone know that story?) This bug alone would have been bad, but not catastrophic...

The problem was that after each successive bounce the return address got longer and longer, until monstrosities like the following became commonplace: <@Macbeth.Stanford.EDU, @Portia.stanford.edu, @Macbeth.Stanford.EDU, @Portia.stanford.edu, @Macbeth.Stanford.EDU:xu@spanky.Stanford.EDU> Once the reply addresses got up to about the length shown in this example, they started to overflow a fixed-length buffer in all Berkeley-derived mails (*no* checking for overflow, of course). This caused the affected mail processes to go crazy. First of all they sent an error message back to the sending machine (causing it to send the viral mail *again* 30 minutes later). Worse, the mangled mail processes continue to run forever until somebody kills them. (And it takes kill -9 as superuser to do it.) One such mail process on a lightly-used Earth Science machine accumulated *9500* minutes of CPU before anyone figured out why the machine had been so slow for the preceding week!

Our first reaction was to scream at the people who run the list, and they said they fixed the problem, but their fix only resulted in a greater variety of mail loops being generated; various interesting orbits about portia, polya, hamlet, macbeth, ... Needless to say as the traffic built up the CPUs and then finally the network itself in the Earth Science department ground to a halt. It became impossible to even log in to many machines to kill the offending mail processes. Killing the processes wasn't very effective, either, since that would not stop Macbeth from immediately starting the whole mess up

again. We finally pulled the plug on sendmail. Fortunately Stanford later had a power glitch that seems to have crashed most of the offending machines, so the network is OK again now. :-)

Newsgroup posting rejected, rejected, rejected, ... (From Earle Ake)

There is a new newsgroup that I subscribe to called vmsnet.announce.newusers. I decided to post a message to it. That is when the fun began. The newsgroup is unmoderated. After I posted to the newsgroup, I received a mail message from a site scolding me for posting to a moderated newsgroup and told me to post directly to the moderator instead. Here is a copy of the message.

"This newsgroup is moderated, and cannot be posted to directly. Please mail your article to the moderator for posting."

It then included my original message to make sure I knew what I had done.

I was going to ignore it until I received 5 more messages from the same site complaining about the same message. I started to wonder, do we have a loop here? I fired a message off to the postmaster at the offending site to stop the messages. A day past and no reply. The messages kept coming in. I started to keep track of how many and how often they were mailed. They were mailed every half hour since I first posted the message. I then looked up the administrators name in the UUCP maps. I sent him a message directly to have him stop these things. He responded by saying he wasn't sure what was happening and to send him a sample of the message so he could fix it. Now we are up to 85 messages. I finally got a response from him saying he had shut them off. It seems one of the sites that he is connected to accepted the message and then tried to hand it off to his site. His version of *news* thinks that any newsgroup that has the word 'announce' in it *is moderated* no matter how you have it set up! The remote site tried every half hour to hand the message off to his site. His site would in turn reject the message and send a nasty gram back to me. We finally got all this straightened out after 140+ messages bounced back to me. I don't think I will post to that newsgroup in the near future!!!!!

Computer bungling of auto insurance premiums: The glitch that stole Christmas (From Barry Kolb)

PGN's calling for RISKS readers to ''play a stronger role in ensuring that our R&D and our educational offerings are suitably concerned with realistic stringent requirements'' is appreciated [Letter From the Editor, ACM Software Engineering Notes, vol. 14, no. 6, October 1989, p. 2]. I often use RISKS examples in class (to demonstrate that the instructor is in touch with the world). In fact, the October 1989 issue of SEN arrived in time to illustrate to a class the need for stringent requirements and testing. As if to underline the point, the following appeared on page A3 of the 1 December 1989 Asbury Park (NJ) Press:

> Computer Error Slashes JUA Surcharges (by Coleen Dee Berry)
>
> Some 18,000 people who get their JUA automobile insurance policies through Computer Sciences Corporation may have thought their premiums were surprisingly less expensive this year.
>
> They were right.
>
> Due to computer error, CSC did not assess bad driver surcharges against about 18,000 of their policyholders. CSC is one of the four new computer companies hired to handle New Jersey Joint Underwriting Association policies.
>
> As a result, CSC has had to advance $3.6 million to the JUA to cover the delayed payments, and last week began notifying those customers to expect a bill for the surcharges. ...
>
> The delayed surcharges were due to a glitch in the CSC's computer system during April and May, when the company was first taking over the JUA account. ...
>
> The move to computer companies was undertaken because it was thought to be cheaper and more efficient, according to state insurance officials.

Unsafe French software (From A. N. Walker)

According to "The Sunday Correspondent" [a new 'quality' weekly] of 3 December 1989, ''Nuclear experts fear that reactors along the northern coast of France have fundamental design faults that could lead to a disaster which could devastate large areas of Britain. ... British experts are also concerned about the increasing reliance being placed by French nuclear engineers on computers whose tasks are so complex they can never be checked for safety. ...'' (page 1).

The inside story, page 3, concentrates on engineering problems with the French PWR reactors, but there appear to be also some computer RISKS:

"Key computer safety scheme error prone

French nuclear engineers are programming their computers using a language which is notorious for allowing dangerous errors to slip in, say British experts. ... Although computer equipment is now highly reliable, the incredible complexity of the software they [sic] run makes it very difficult to guarantee their behaviour ... Professor John Cullyer, of Warwick University, ... says ... [the complexity] is "beyond present capabilities". The French nuclear industry's wide use of a computer language called C is also criticised by [unnamed -- ANW] British software experts. They claim that it is too easy to write dangerous programs with C, yet difficult to spot the mistakes .... [A French spokesman said ...] "Yesterday we had a demonstration for visitors and everything worked fine".

Another foretaste of the Millenium (From Brian Randell)

The university computing service at Newcastle runs MTS (the [Michigan Terminal System) on an Amdahl mainframe, which crashed mysteriously, as did various other MTS sites in North America, hours later. The explanation is given in the following message from a system programmer.

> We apologise for the unexpected system shutdown today (Thursday). This was caused by a bug in the MTS [Michigan Terminal System] that was a "time-bomb" in all senses of the word. It was triggered by today's date, 16th November 1989.
>
> This date is specially significant. Dates within the file system are stored as half-word (16 bit) values which are the number of days since the 1st March 1900. The value of today's date is 32,768 decimal (X'8000' hexadecimal). This number is exactly 1 more than the largest positive integer that can be stored in a half-word (the left-most bit is the sign bit). As a result, various range checks that are performed on these dates began to fail when the date reached this value.
>
> The problem has a particular interest because all the MTS sites world-wide are similarly affected. Durham and Newcastle were the first to experience the bug because of time zone differences and we were the first to fix it. The American and Canadian MTS installations are some 4 to 8 hours behind us so the opportunity to be the first MTS site to fix such a serious problem has been some consolation. The work was done by our MTS specialist who struggled in from his sick bed to have just that satisfaction!

[I presume the MTS folks did not read the earlier RISKS item in *SEN* 14 6 and RISKS-9.28, "Hospital problems due to software bug", in which we learned that 19 Sept 89 was 32768 days after 1 Jan 1900! This problem can be expected to recur in one guise or another... PGN]

New Year's Lotto goes Blotto

The Pennsylvania Wild Card Lotto computer systems had already been reprogrammed to accommodate the end of the decade, but apparently the software maintenance was not done carefully enough. In the first Lotto of the new decade, the computer systems were unable to determine the winners and further fixes were required. [Philadephia Inquirer, 4 Jan 1990, contributed by James P. Anderson]

Hardware failure mimics hackers (From Rob Wright)

Two systems - same day, same symptoms. Hackers? No, hardware!

20 September 1989, Bentley, Western Australia, Curtin University of Technology.

The VAX-11/750 computer in the Geophysics Laboratory refused to allow any user to log in. All passwords, including *system* were declared invalid. The system manager contacted me and I showed him how to break in. There appeared to be some disk damage, but after setting all passwords to known values, the system was apparently usable. Shortly thereafter all was not well. Indeed, after any two users were logged in the system refused further logins, complaining that the licensed number of system users had been exceeded. Given that this particular machine (running VMS 4.7) has never been a microVAX, the only class of system which imposed such a limit, I naturally suspected foul play. At this stage I was sure that the system had been hacked, and was recommending a total re-installation of all the software, starting from known, reliable distribution tapes.

[Extensive subsequent discussion appeared in the on-line RISKS Forum. The bottom line was a flaw in the hardware floating point accelerator, which was used for password 'encryption' and which also caused multi-user licensing to fail. PGN]

Courts say violation of professional code is malpractice (From Jon Jacky)

Excerpts from 'Malpractice in IS?', by J.J. Bloombecker, *Datamation*, 15 October 1989, pp.85-86:

A ruling by a US Court in Missouri ... recognized computer malpractice as the basis for holding third-party IS practitioners liable for acquiring an unworkable computer system for a client ... In *Diversified Graphics v. Groves*, the

jury held consultants from Ernst & Whinney (Now Ernst & Young, having merged with Arthur Young and Co.) liable for shirking the Management Advisory Services Practice Standards of the American Institute of Certified Public Accountants (AICPA) in their procurement of a turnkey system for Diversified Graphics. In February, the US Court of Appeals of the Eighth Circuit agreed, and it let the jury verdict stand. "*Diversified* is a significant precedent for [establishing] the proposition that liability can by incurred by any professional performing the types of services that E&W offered to perform," says Peter Sadowsky, a partner in The Stolar Partnership in St. Louis, which represented Diversified Graphics. "It is equally likely to apply to people doing systems design or programming, not just systems acquisition." ...

"Prior to *Diversified Graphics*, most courts refused to extend professional liability standards to computer specialists. Now we've got a federal court of appeals doing just that," said J.T. Westermeir, a partner in the Washington DC office of Fenwick, Davis and West, and a specialist in computer law. Furthermore, says Westermeier, an IS manager who lists membership in an association such as DPMA or ACM on a resume implies that he or she has accepted the associations professional standards. Having done that, a computer professional should expect his or her work to be judged by those standards.

Other lawyers who have analyzed the case, however, say it is unclear whether professional standards for IS managers could be used as a similar basis as the AICPA standards were in *Diversified*. John Hennelly, a partner at Bryan, Cave, McPheeters and McRoberts in St. Louis, which represented Ernst & Whinney, says the case doesn't necessarily lead to broader conclusions about the liability of nonaccountants ... Eric Savage, with the Hackensack, N.J.-based law firm of Michael Goodman, believes it was easy for the court in *Diversified* to find E&W guilty of malpractice because of the accounting organization's highly visible professional standards. Thus, he says, it would be difficult to apply the decision to a case that is adjudicating the liability of a computer professional not employed by an accounting firm. ...

(There are two sidebars to the story. One, labelled 'A Case In Point', describes the client's needs, and how the system recommended by the accounting firm failed to meet the client's needs. This sidebar quotes the court's finding that the accounting firm did not have sufficient expertise to recommend a computer system for this client. Another sidebar, 'How Some of the Standards Compare', quotes the relevant portions of the AICPA Standards, which essentially say that members shall only accept jobs which they are qualified to perform, and shall conscientiously perform the jobs which they have accepted to the benefit of their client. This is placed alongside sections from the Association for Computing Machinery (ACM) Disciplinary Rules which essentially say the same thing.) Jonathan Jacky, University of Washington

SUBSECTION ON COMPUTERS IN ELECTIONS

"Computer Error" in Durham N.C. election results (From J. Dean Brock)

According to 'Computer Twists Election Results', 9 November 1989, Durham Morning Herald, a "computer error" caused eight precincts to be counted twice. The correction actually changed the result of one city council race twelve hours after it was assumed settled. It's difficult to determine the nature of this computer error from the newspaper article.

Another front-page article entitled 'Haywire Machine Counted Precinct Vote Totals Twice' quotes Jo Overman, the chairman of the County Board of elections, as saying: "One terminal used Tuesday apparently counted twice each precinct entered into it.... What was called in was correct, the computer just added it twice.... It was not added by an operator, it was a glitch in the program." Ms. Overman, also added that the "errant terminal was an extra unit put on election duty as part of a last-minute effort to process returns faster."

Interestingly, the precinct-by-precinct breakdown given to the media was correct, even though they did not match the totals. The mistake was discovered in a later hand check of the results by the Board of Elections. Apparently, no one else bothered to check the totals.

The director of the county's Management Information Services department, which would be responsible for any programming errors, was instructed by the elections supervisor not to say anything about the election.

(From Ronnie W. Smith)

The only information I have to add is that the local TV media kept referring to it as a "computer error" without ever mentioning that the original source of the error was a person. The newspaper never explicitly made this link, but at least mentioned it was a programming error. Interestingly enough, the man who became the winner after he had been declared the loser did refer to it as a "human error". The number of votes that had been double added was slightly more than 6000.

(From John A. Board)

[...] I find it most fascinating and troubling that it took over a day for anyone to notice that the correctly reported precinct votes duly tabulated in the paper the morning after the election did not add up to the numbers reported as totals at the bottom of the columns, and the errors were not small - the Mayor's race vote, for example, had been reported as 19,381 to 17,118 when in fact the real totals of the votes as listed were 16,136 to 13,356! To the credit of the elections board, the errors were apparently found during manual verification of the automatically reported "unofficial" results.

Glitch in Virginia election totals (From Paul Ammann)

In the 7 Nov 89 Virginia gubernatorial race, Doug Wilder (D) defeated Marshall Coleman (R) in a close race. At one point out of a total of 1.7 million votes, AP reports a difference of 5,533 votes and UPI reports a 7,755 vote gap. A Washington Post article (9 Nov 1989, pp. A37, A40) discussed the reasons for the discrepancies and the mechanism for official vote tallies. Buried within that article was the following gem: ... For an hour on Tuesday, [AP's director of planning Evans] Witt said, a computer glitch caused some of Wilder's votes in predominantly black precincts to be counted twice; the error was fixed and the vote total was adjusted. ... AP's Witt said that "there's almost always a variation between the official and the unofficial count," but said he could not think of an instance in which the results of an election had been reversed because of a mistake by the wire services. [Vote Counting Methods, Race Factor in Polls Leave Plenty of Room For Error Disparities Remain in Va. Governor's Race Tallies, By Stephen C. Fehr, Washington Post Staff Writer>

Rome: Operator error causes publication of wrong election results (From Lorenzo Strigini)

On 29-30 October 1989 elections were held in Rome for a new city administration. Unofficial results published at first gave an important victory to the Christian Democrats, but at the end of the tallying this victory almost vanished. The publication of wrong results was attributed to a data-entry operator error. Since then, the political parties have been exchanging accusations of intentionally manipulating the data for political advantage (the supposed advantage would be a short-term boost in popularity for the Christian Democrats, or casting suspicions on the Christian Democrats, for the Communist). To set things in context: besides deciding who will manage the capital city of Italy, these elections were regarded as an important indicator for national policy, and the major parties had put much effort in a combative, venomous campaign.

Now the details. (Disclaimer: this is my interpretation, checked with a few colleagues, of very imprecise press and radio reports. ...)

Voting and vote counting are by hand, with paper ballots. After the count started, and as partial results were transmitted from the individual "electoral sections", an EDP center of the City of Rome added them to obtain partial accrued results (without official value) and transmitted them to the press, radio and TV.

Very soon in this process, the published results showed a marked gain for the Christian Democrats. Later, it turned out that a few tens of thousands of extra votes had been erroneously given to them. The error became evident because the sum of the votes was greater than the number of voters. In an interview, the director of the EDP center stated that he had received from the computer program warnings about the discrepancy, but had ordered the publication of results to continue, assuming the problem was temporary and it would disappear later on.

Two days ago, the operator was found that allegedly caused the problem. He had to type in a screenful of data, send them to the computer and wait for it to clear the screen and prompt for new data (or to unlock the keyboard?). He found that pressing a certain combination of keys allowed him to clear the screen and restart input sooner, so speeding up his work. But by this trick he sent wrong data ("this affected the votes for 4 parties, and in particular the number of votes for the Christian Democrats -line 18 on the screen - was substituted with the number of the electoral section"). The program would complain about receiving inconsistent data, but give him an override option, which he used.

Now my comments. Funny: everybody is complaining about evil intentions (of which there's no proof), not about incompetence. From the news stories, some technical/organizational flaws are evident:

- The input routines checked for transmission overruns, or the application program ran consistency checks on each individual transaction (the entering of the results from a given number of ballots) but allowed the operator to override them (there was a log of the override requests, though: all inputs were logged to tape; but the log of part of the session was lost because tapes were scarce, and some were used twice).

- The director of the EDP center ignored the warnings (it is unclear whether these were from a global auditing of the data base or were the same error messages sent to the operator) about inconsistent data.

But, most important: in their greed for early results, both the press and the politicians trusted a non-trustworthy system. It appears that the only checks applied to this unofficial counting procedure were the consistency checks mentioned. If one were to bribe the operators to shift votes *consistently* from one party to another, this could go undetected until the official tally was available, several days later. The vulnerability so created is great: news reports of, say, an 80% victory of the Communist Party would certainly hit the Stock Exchange hard; the resulting allegations of fraud would cause a political earthquake (in the '50s, they might well cause a civil war). As things are, the effect on the public appears quite serious: according to an opinion poll, some 30% of the voters interviewed said that, if the election were held again after the news of the mix-up was known, they would refuse to vote. [Lorenzo Strigini, Istituto di Elaborazione dell'Informazione, Pisa, Italy]

[Regarding greed for early results, it was interesting to note that the advance polls in the New York City mayoral race were off by roughly 11%, and the exit polls were off by 10%. PGN]

"Play it Again, Yonkers" -- more election funnies (From Steve Bellovin)

There was a very close, and racially-charged, mayoral election in Yonkers, NY in November 1989. The challenger was rather unexpectedly reported the victor by 4,000 votes on election night. When the official tally was started, though, the incumbent had picked up 1,500 votes in just 5 of the 12 precincts. The count was suspended for the weekend, with the voting machines impounded; when it was finished, the original result -- and numbers -- were upheld.

What happened? It's an old story here, I'm sure. Before the election, the tally program was run with test input data. They forgot to take out the test data when tabulating the real returns. From the story I heard, it wasn't clear if the error was in the official tally or in the early returns; given the numerical result, I tend to suspect the former. Steve Bellovin

Vote counting problems - experience in Michigan (From Lawrence Kestenbaum)

I have followed with interest the recent discussions of vote-counting errors in Durham NC, Yonkers NY and elsewhere. Perhaps the following may be of interest. It is a discussion of a specific vote counting problem in a jurisdiction where I served until last year as an elected official.

Some of the recent problems with inaccurate election-night vote tallies can be traced to the badly-handled interface between computer and manual systems. Non-electronic vote counts, for example, are mistyped on computer screens during the hectic atmosphere of election night. Of course, when the computer system plays the dominant role, the difficulties with the non-computerized parts are even greater.

While most of the Northeast still votes on the old-style lever machines, the Midwest -- Michigan at least -- has largely moved to computer punch card ballots. Punch cards have certain advantages: in the event of a recount, a tangible, anonymous record exists of each voter's choices. By contrast, recount lawyers are often able to find whole voting machines whose votes must be excluded from the count because of mechanical problems, thus disfranchising anyone who voted on that machine. Other problems are possible, but all in all, results from punch card jurisdictions are regarded as being much more 'firm' and resistant to being altered in recounts and challenges. At the same time, it lulls political people into a sometimes unjustified faith in computer-generated vote tallies.

When I served on the county board in Ingham County, Michigan (1983-88), we had a mixed system. The choice of voting method was made individually by the 21 townships and cities within the county. Thanks to strong persuasion by the county clerk, almost all of the 250 or so voting precincts in the county voted on punch cards. The remaining five precincts, in four small jurisdictions, used voting machines; absentee voters in those five precincts used punch cards. In no other part of the county were absentee votes counted separately. Under contract with most of the punch-card jurisdictions, the county provided the materials and organized the ballot counting process.

The software which aggregated and reported the votes for the county, and also automatically generated all of the official statements to be attested to by the Board of Canvassers, did not allow for the entry of non-computer precincts. Thus, the county clerk's people had to break into the program and override its security features in order to input the numbers for the five rogue precincts. The risks here should be obvious! Invariably, this task was postponed until very late at night, when the operators (who normally worked 8am to 5pm) were extremely tired. More than once, as I recall, this led to errors in the overall totals, though none which changed the outcome, and all were corrected by the following day.

After a few years of this, the county clerk (with full support from the county board) mounted a major effort to corral the five remaining precincts. He succeeded with all but one of them, the City of Leslie. So, on a smaller scale, the problem -- and the risk -- continues. Lawrence Kestenbaum

[Lawrence Kestenbaum's message gives an interesting first-hand account. However, there is much debate in the election computing community about the relative tamperabilities of machine-readable cards (punched or mark-sensed), lever machines, and direct-entry screen menus. Punched cards give results that are more or less repeatable (ignoring the hanging chad problems). But they are subject to tampering *before* any votes are ever tabulated (removed cards, added cards, multipunched cards, hidden prepunches, trick punches that unleash Trojan horses, etc.), which can make the repeatability argument moot. The recount would mask the prior fraud and even add apparent credibility! The fantasy that there is a *correct* anonymous physical record is very tricky to convert into a reality. (There are different vulnerabilities in the other types of systems, such as the presence of perfectly repeatable but hidden and probably undetectable Trojan horses in the direct-entry systems -- especially in proprietary systems. See earlier issues.) PGN]

Computerized voting machine misbehaves (From Rodney Hoffman)

The 3-Dec-89 "Los Angeles Times" carried a story by Paul Houston headlined 'Computerized Vote Tallies Have Too Many Glitches, Experts Charge'. The bulk of the story was a review of criticisms of these systems, pegged to last month's close gubernatorial election in Virginia. The article cited Mae Churchill of Los Angeles-based Election Watch, Computer Professionals for Social Responsibility, Roy Saltman (NIST) and Robert Naegele, a San Jose computer consultant.

The final paragraphs of the article related a miserable demo:

... one of Fairfax County's (VA) 600 Shouptronic machines fouled up in a demonstration for Los Angeles Times reporter William Trombley last May. "The machines have worked very well," Jane G. Vitray, secretary of the county board of elections, said as she prepared to demonstrate one of the machines to Trombley. But the machine that prints out the names of candidates and issues -- the information that appears on the face of each machine -- printed everything in Italian. The ballot plotter also prints in French, German, and Spanish, as well as in English. "We didn't know it did that," Vitray said with some annoyance. "We didn't want that feature."

While an aide was left to deal with the language problem, Vitray and the reporter moved on to the voting booth, where bells were chiming and red lights were blinking and an inviting green button at the bottom right corner of the machine said "vote." "Don't push that," Vitray warned. "Once you push that, you can't vote for anything else. You only push that button when you're finished." In a previous election, a number of voters had pushed the green button too soon and then "called to tell us we were depriving them of their constitutional right," Vitray noted.

After Trombley finished voting, another red light came on to indicate that the result had been printed on a tape at the back of the machine. But when he and Vitray checked the tape, it was empty. Vitray was exasperated. "I can't understand it," she said. "Everything worked so well last week, when the Girl Scouts were here."

Stuffing the electronic ballot box (again)

Charles Schwab & Co spent more than $100,000 to conduct a nationwide poll on program(med) trading, with two widely advertised free 800 phone numbers set up to record the pro and con votes. Apparently someone at Wells Fargo (which has a high-profile program trading subsidiary) set up an autodialer to vote YES continuously, which was detected by their programmed monitoring. (' "First we have program trading. Now we have program dialing," quipped Senior Vice President Hugo Quackenbush. ') In 12 hours, there were 12,191 votes, 65.3% for, 34.7% against. [Source: San Francisco Chronicle, 11 Nov 1989, pp. B1-B2.]

[By the way, I observe that one call every twenty seconds for 12 hours would account for the entire difference between the pros and cons. One call every six seconds would have accounted for ALL of the pro calls. We might suspect that an autodialer could easily have skewed the results -- although perhaps others on both sides were also using the same strategy.]

SUBSECTION ON COMPUTER SECURITY

Computer Viruses Attack China (From Yoshio Oyanagi)

Ministry of Public Safety of People's Republic of China found this summer that one tenth of the computers in China had been contaminated by three types of computer virus: "Small Ball", "Marijuana" and "Shell", China Daily reported. The most serious damage was found in the National Statistical System, in which "Small Ball" spread in 21 provinces. In Wuhan University, viruses were found in *all* personal computers. In China, three hundred thousand computers (including PC's) are in operation. Due to premature law system the reproduction of software is not regulated, so that computer

viruses can easily be propagated. Ministry of Public Safety now provides "vaccines" against them. Fortunately, those viruses did not give fatal damage to data. [Yoshio Oyanagi, University of Tsukuba, JAPAN]

First Virus Attack on Macs in Japan (From Yoshio Oyanagi)

Six Macs in University of Tokyo, Japan, were found to have caught viruses, newspapers and radio reported. Since this September, Prof. K. Tamaki, Ocean Research Institute, University of Tokyo, has noticed malfunctions on the screen. In October, he applied vaccines "Interferon" and "Virus Clinic" to find his four Mac's were contaminated by computer viruses, "N Virus" type A and type B. He then found ten softwares were also infected by viruses. A Mac of J. Kasahara, Earthquake Research Institute, University of Tokyo, was also found to be contaminated by N Virus and Score Virus. Those are the first reports of real viruses in Japan.

Later it was reported that four Mac's in Geological Survey of Japan, in Tsukuba, were infected by N Virus Type A. This virus was sent from U. S. together with an editor. [Yoshio Oyanagi, University of Tsukuba]

"Computer Virus Countermeasures" Article (From Will Martin)

Readers of RISKS might be interested in a rather strange article in the October '89 issue of DEFENSE ELECTRONICS, p. 75, entitled "Computer Virus Countermeasures -- A New Type Of EW" [EW = Electronic Warfare], by Dr. Myron L. Cramer and Stephen R. Pratt (both of Booz, Allen & Hamilton, Inc.).

The reason I consider this "strange" is because the whole thrust of the article is how computer-based ECM [Electronic CounterMeasures] and EW systems could be infected by viruses which are transmitted over the air and enter those systems or their components via the normal sensing channels -- that is, they would pick up a digital stream the same way they would pick up an enemy radar signal, and that digital stream would contain code which would somehow find its way into the executable code for the system's processor(s).

> This is the electronic analog of the program trapdoor through which a Trojan horse, worm, or virus could be installed. The *sendmail* debug option and the *gets* missing bounds check are recent reminders of the nature of the problem. Out-of-band signals could also be used to trigger trapdoor effects. Furthermore, whether these effects result from an accidental flaw in the system or a preplanned Trojan horse program that would wait for the attack to be triggered, the results could be serious in either case. PGN

McRisks - Electronic Interference in Fast Food Automation (From Robert Horvitz)

"The Importance of EMC in the Preparation and Selling of Big Macs," by Fernando M. Esparza is a fascinating article in the September-October 1989 issue of "EMC Technology." (EMC = Electromagnetic Compatibility, the science/art of getting electronic devices to work properly without interfering with one another.) Esparza, the author of McDonalds' "Electrical Disturbance Standards," has some great war-stories to tell about problems cropping up in these highly automated fast-food environments due to unforeseen interactions among appliances. One he described as "the most serious interference incident that McDonalds has ever experienced" involved toasters and timekeeping.

It seems that when McDonalds decided to introduce McMuffin products, they had to install special toasters. Soon, many of their employee time-clocks inexplicably started to gain 2 to 4 hours each day, crediting workers with more hours than they had actually worked. After a lot of head-scratching (and testing), they discovered that the new toasters' voltage control circuits induced voltage spikes in the powerline during normal operation - sometimes as many as 120 per second. This disrupted the clocks on the same power circuit, since they monitored the alternating current's waveform for the purpose of time-keeping: the voltage spikes increased the number of "zero-crossings," which were used as the metric. "By the time we were able to pin down the problem exactly, there were more than 5,000 toasters installed in the restaurants... Some restaurants reverted to manual procedures for payroll timekeeping, but there were a number of employees who were paid for extra time because of the clock errors. Although the managers were understandably upset, none of the crew complained."

"Ghosts in the Drive-Thru" was another baffling problem, affecting the POS (point-of-sale) system of a McDonalds in suburban Los Angeles: "The POS system is a collection of computerized cash registers that are networked together in a somewhat sophisticated and proprietary network," Esparza explains. The problem was that bogus food orders showed up randomly in the system. "The restaurant could distinguish ghost orders from real orders because the quantity of the items displayed was the same - 11 cokes, 11 fries, 11 hamburgers, etc. The items themselves were directly copied from the previous, actual order. These orders could not be cancelled but had to be cashiered out of the system, thereby rendering all product mix and sales information invalid and creating a potential security/theft problem, in addition to slowing customer service in the drive-thru."

The restaurant's POS system and all of its software was replaced, but the problem continued. To make a long story short, this McDonalds happened to be near a cluster of radio and television transmission towers. The POS system's wiring acted as an antenna, capturing the signals, and corrupting some of the data that flowed thru the wires.

One problem described in this article stands out as a potential threat to many more retailers than just McDonalds: "The Cash Drawers that Opened by Themselves." Again making a long story short, Esparza discovered that the problem began soon after the local police department upgraded their communications system with higher-power mobile radios. "Whenever they responded to a call while in the drive-thru, the cash drawers opened... An open cash drawer without a cashier to supervise it is...a large security liability."

["EMC Technology" is a controlled circulation bimonthly. Subscriptions are free to those who qualify, $40/year for those who don't. For more information contact EMC Technology Circulation Dept., 5615 West Cermack Rd., Cicero, IL 60650-2290 USA.]

Offensive message on electronic information board (From Bob Morris)

Offensive Message Flashes at Busy City Corner
By Linda Wheeler, Washington Post, October 25, 1989

An offensive message that mystified the owners of an electronic information board was flashed Monday at Connecticut Avenue and L Street NW, one of the city's busiest intersections.

A Georgetown University law student, Craig Dean, said he saw the message *'Help Stamp Out A.I.D.S. Now: Kill All Queers and Junkies'* flash five times in 25 minutes. Minutes after seeing the message, he called the city Human Rights Office and the Washington Blade, a gay community newspaper. Doug Hinckle, a staff photographer for the Blade, saw the message flash once and photographed it. ... Judith Miller, president of Miller Companies, which own the building at 1101 Connecticut Ave. NW and the message board, said she did not know how the statement got onto the board. She refused to believe it had appeared until told of the photographs. Her company has complete control of the board and does not accept any paid messages or advertisements, Miller said. "I would never do anything like that," she said. "There is no way I would allow such a statement to appear."... Yesterday, Keller, a five-year employee of the Miller Companies, said he did not write the statement and does now know how it became part of the normal flow of headline news. Miller said she believes her computer system may have a "virus" and will have experts search to find where the unauthorized statement originated. "How absolutely awful," she said of the message. ...

[Also noted by John Crider, who added: Possibly another case of how media-induced heightened awareness, this time about viruses, can lead to the emergence of a new scapegoat; years ago the operator would have been fired on the spot, but now it's a viral infection. Both are knee-jerk reactions - conclusions should come *after* the facts are examined. John Crider]

14-year-old cracks TRW credit for major fraud (From Rodney Hoffman)

Condensed from a story by Jennifer Warren in the 'Los Angeles Times' 18 October 1989:

A 14-year-old Fresno, CA boy obtained secret "access codes" to the files of TRW Credit from a bboard and used them to pose as a company or employer seeking a credit history on an individual whose name he picked randomly from the phone book. From the histories, he obtained credit card numbers which he then used to charge at least $11,000 in mail-order merchandise (shipped to a rented storeroom) and make false applications for additional cards. He also shared his findings on bboards.

Police began investigating when TRW noticed an unusual number of credit check requests coming from a single source, later found to be the youth's home telephone number. The high school freshman, whose name was not released, was arrested at his home last week and later released to his parents. His computer was confiscated and he faces felony charges that amount to theft through the fraudulent use of a computer.

"Here's a 14-year-old boy with a $200 computer in his bedroom ... and now he has shared his data with countless other hackers all over the nation," said Fresno Detective Frank Clark, who investigated the case. "The potential [for abuse of the information] is incredible."

Hackwatch spokesman charged (From Dave Horsfall)

This item, taken from "Computing Australia", 2nd October 1989, should warm the cockles of a few hearts...

"Hackwatch spokesman charged

Self-styled computer security expert Paul Dummett, alias Stuart Gill, has been charged with making false reports to the Victoria Police following an investigation into claims he made in the daily media late in 1988 and early this year. The articles often quoted Gill, introducing himself as a spokesman for either "Hackwatch" or the "DPG monitoring service".

Gill claimed hackers in Australia had gained access codes from others in the US and lifted $US500,000 from the International Citibank, US. Other claims: credit card numbers had been posted on bulletin boards for BBS users' access; drugs, including steroids, were being sold using bulletin boards; evidence of this had benn given to the police by informers; and in response, the police had raided several hackers' homes. The police, including the Criminal Investigation Bureau and the Fraud Squad's Computer Section, repeatedly denied the claims.

Gill had disappeared, but returned again on September 22 and was charged in the Frankston Magistrates' Court under his real name, Paul Dummett. According to court documents, police investigating Dummett's claims allegedly found Citibank's computer network had not been illegally accessed on its New York number as Dummett had claimed. When Dummett appeared in court his legal aid counsel Serge Sztrajt applied successfully to adjourn the case to October 20. Dummett did not enter a plea."

CERT Advisories

The on-line RISKS Forum included detailed advisories on (1) DEC/Ultrix 3.0 breakins using tftpd, weak passwords, and known unpatched security holes, (2) the DECnet 'WANK' Worm on SPAN that affects DEC VMS systems, and (3) a SunOS 4.0.x rcp problem, which can be exploited by other trusted hosts listed in /etc/hosts.equiv or /.rhosts (fixed in 4.1). For details, contact the CERT (Computer Emergency Response Team) at cert@sei.cmu.edu or 412-268-7090 (24-hour hotline).

Marshall Williams convicted of destroying data

Marshall Williams, a former company cost estimator for Southeastern Color Lithographers Inc., Athens GA, was convicted on 16 Nov 89 for "using his company's computer network to destroy billing and accounting data as well as backup copies of that data". A key piece of evidence was a computer audit trail of data-deletion commands that traced deletions to his terminal. The defense raised the potential for a frame-up resulting from someone tampering with the audit trail data. (No one seems to have suggested that someone else might have been using his terminal.)

The crime allegedly cost Williams' former employer more than $400,000 in lost business and downtime. He faces up to 15 years in prison. Williams contended that he "knew nothing about his employer's complicated Xenix operating system and could not have deleted the data." He plans to appeal. [Source: PC Week, 27 November 1989, p.1, article by Richard March]

Kevin Mitnick's accomplice sentenced (From Rodney Hoffman)

Leonard DiCicco was once a friend of convicted hacker Kevin Mitnick (see *SEN* 14 6). In July 1989, DiCicco pleaded guily to charges of permitting Mitnick to gain access to a computer at DiCicco's workplace last December, which was then used to steal a $1-million DEC security software program.

According to a small notice in the *Los Angeles Times*, 30 November 1989, DiCicco has now been sentenced to 5 years' probation, plus 750 hours of community service, part of which will be spent installing a computer system at a shelter for the homeless.

Desktop forgery (From Rodney Hoffman)

"Desktop Forgery", by David Churbuck, is the cover story in the 27 November 1989 issue of *Forbes*. It tells how to scan in a check, alter it, print it, and pass it (with a few details omitted), and it tries to frighten bankers and others with the endless possibilities.

Churbuck does note, "To be sure, the desktop computer did not create the crime of forgery. All it did was make the tools user-friendly. Check-passers can now practice forgery in the privacy of their own homes...."

The Trojan horse named 'AIDS' (From Evan "Biff Henderson" Eickmeyer)

The following article is from the Los Angeles Times, 15 December 1989, p.D3.

AIDS Data Disk Has PC-Damaging Virus, by Michael Specter, The Washington Post

A mysterious computer diskette about AIDS that was mailed to major corporations, insurance companies and health professionals across the world contains a hidden program that has destroyed information in thousands of personal and corporate computers, police in London said Thursday. Officials of Scotland Yard said at least 10,000 copies of an unusual "AIDS Information Diskette," which promised to help users deduce their risk of becoming infected with the AIDS virus, were sent to people in England, Scandinavia, Africa and the United States. Hospital systems from London to Stockholm reported damage Thursday and AIDS researchers at major institutions in the United States, from the National Institutes of Health to the University of California at San Francisco, issued alerts to all their computer users.

"Extremely urgent message for all National Institute of Allergy and Infectious Disease PC Users," said a flyer sent Thursday to AIDS researchers at NIH. "A diskette from PC Cyborg Corp. contains a highly destructive virus. All systems running these programs had ALL hard disk data DESTROYED." Neither that corporation nor Ketema Associates, its parent company, has any known officers or location, according to people who tried Thursday to find them.

In Sweden, the State Bacteriological Laboratory sent letters to clinics and doctors warning them of the diskette. Chase Manhattan Bank was one of the first companies to report problems with the diskette, which also was sent to the London Stock Exchange, British Telecommunications, Lloyds Bank, the Midland Bank, other major banks and manufacturing companies. "We have never seen anything approaching the magnitude of this attack," sand John McAfee, chairman of the Computer Virus Industry Assn., though he noted no damage had yet been reported in the United States. "It took enormous preparation, coordination and a huge amount of money."

People familiar with computer "viruses" and other computer "diseases" were baffled by the maliciousness of the crime, the amount of money and sophistication it required and its lack of any immediately discernible motive. Computer programs written as pranks or tools of minor sabotage have become ubiquitous over the past few years. But this one was different, according to experts across the country. The diskette came in a slick package mailed from offices on London's tony New Bond Street. The bright blue cover sheet said the package contained AIDS information, and informed recipients that the information was easy to use and would help them calculate the risks of exposure to the disease.

[Further details on this case were distributed on the on-line RISKS and VIRUS distributions. PGN]

SUBSECTION ON COMPUTERS IN AIR, SPACE, DEFENSE, GOVERNMENT, ETC.

Air Traffic in Leesburg VA

The air traffic on Friday evening, 3 November 1989, around Washington DC was awful. Both the primary computer system *and* the backup were seriously degraded for at least two hours during the evening rush hour, stacking up and backing up air traffic extensively. I heard someone at the FAA mention a buffer overflow (on one system?), but heard no definitive reports. (I did not have to fly out of National until the next morning, by which time all was back to normal.)

Air-Traffic Disruptions at Dallas/FtWorth (From PGN and Robert Dorsett)

For the second time in a week air traffic at Dallas-Fort Worth International Airport was disrupted. The Thursday 19 October computer outage (1950s-vintage computer system) lasted at least twelve hours, and caused delays. [Source: Washington Post, 21 Qct 89, p22]

FAA officials said Thursday's breakdown happened when one of four data processors on the computer failed to start after routine maintenance. The processors feed specific information about each plane from the radar to the controllers' screens. Flights continued at a reduced rate during the outage.

The previous week's outage, on 14 Oct 89, lasted for 19 minutes. It was traced to a technician who mistakenly tried to program a radar computer from the wrong terminal.

Tony Dresden, a spokesman for the National Association of Air Traffic Controllers, said the FAA is trying to upgrade computer systems across the country. But the process is painstakingly slow, he said. "I think if you go to any terminal across the country you'll find some older equipment mixed in with some new equipment," Dresden said. "So this is not just confined to terminals at the Dallas-Fort Worth airport, but to terminals across the country."

Norm Scroggins, tower manager at D/FW airport says the FAA is looking into the problem. "We're in an interim mode," Scroggins said. "I don't think it's particularly useful that any government agency is unable to stay up with the technological industry. It's just hard to get the stuff in. "And you have to keep in mind that this same equipment is

working quite well in Houston. They just don't have the demands that we (D/FW) have."

[Excerpted by PGN from an article from the The Austin-American Statesman, 21 Oct 89, provided by Robert Dorsett]

USAir 737-400 crash at LaGuardia

At the very end of an article in the 22 Sep 89 San Francisco Chronicle from the NY Times ("Cause of Accident a Mystery; Probers Can't Find Pilots in USAir Crash") is this:

"Aviation experts said the controls of the 737-400, a modified and modernized version of a plane that has been one of the most reliable in commercial aviation for many years, are unusual in that they are integrated with computers. Instead of pushing a throttle to accelerate, a pilot uses a computer-like keyboard to enter in a set of commands that set the power of the engines on takeoff. It is possible, experts said, that an erroneous set of numbers was entered and that this accounted for the insufficient power on takeoff."

Earlier in the article was this:

"... the pilot had flown the planes for only two months, and the co-pilot was said to have been in a 737 cockpit for the first time. ... initial reports indicated that the co-pilot was at the controls during the take-off ... the co-pilot told the Port Authority police shortly after the crash that the pilot had been "mumbling" and "acting irrationally" just before takeoff."

[Saturday's and Sunday's papers stated that officials had indicated that a wrong button had been pushed, although Sunday's paper suggested that there might have been mechanical failure as well... The pilot and copilot have been suspended for disappearing afterwards.]

Varig 737 crash in the Amazon (From Dave Horsfall)

Taken from "Computing Australia", 9th October 1989:

Missing zero blamed for aircrash

Brazilian crash investigators have concluded that a data input error caused the Varig Boeing 737 disaster that killed 12 people last month. Pilot Cezar Augusto saved the lives of 54 passengers by ditching his aircraft in the Amazon jungle tree tops after running out of fuel.

An investigating team from Rio de Janeiro believe Captain Augusto miskeyed his computer-controlled flightpath on take-off, omitting the first zero from his true course of "0270" when en route to Mexico. The computer navigation system directed the aircraft south instead of north without the crew realising until it was too late.

The findings have been slammed by the Brazilian Airline Pilots' Association which says the true fault lay in the computer. A spokesman for the association said it had evidence that a flight course computer print-out had detailed the wrong course. The association is calling for a re-examination of Rio de Janeiro Airport's flightpath-mapping system to check on its safety.

Software reliance/software problems and the Stealth (From Marc Rotenberg)

The Washington Post has run an extraordinary three-part series on the development of the Stealth bomber and the subsequent political turmoil as the project faces increasing public scrutiny and Congressional skepticism. The article was written by Rick Atkinson and appears in the 8, 9, and 10 October 1989 issues of the Post.

... "Because of the unique, three dimensional computer design system, Northrop felt confident enough to skip the usual step of building master tools for a bomber prototype; instead, AV 1 [Air Vehicle 1, the first B-2 off the production line] would be a full production plane built with the same 'hard tooling' used on the rest of the fleet. Boeing and Northrop tested internal aircraft systems, such as fuel and hydraulics, on huge 'Iron Birds' that resembled full-sized bombers with their skins peeled away. Beginning in 1985, navigation and avionics equipment was tested in the air of NKC-135 aircraft flying out of Edwards Air Force Base in the Mojave Desert.

"Northrop believed that it could reduce the number of construction man-hours from 3.5 million on the first bomber to 1 million on the 11th. New aircraft often are plagued with production gremlins; those hiding in AV 1 caused another six months of delay. A computer software miscalculation meant that electrical wiring had to be done over because the first set of wires was cut too short, according to a former Northrop executive; a pressurized line blew out an took two weeks to fix because it lay in an inaccessible cranny of the plane." ... [Excerpted from the 10 October issue].

Murphy's Law Meets the Navy

The Navy has an elaborate safety program that includes extensive concern for safety in computer-controlled systems. Unfortunately there is an apparent gap between the intent and the execution overall. For the record, here is a summary of the two weeks period leading up to the two-day mid-November global reorientation. It may be worth noting that none of this run of problems seems to have been blamed on computers, but then most of our so-called "computer problems" are people problems anyway, irrespective of where the blame is placed.

- 29 Oct. Pilot's first-ever carrier landing kills 5 on carrier Lexington.
- 30 Oct. FA-18 pilot drops 500-pound bomb on guided missile cruiser Reeves; 5 injured.
- 31 Oct. Wave washes 3 sailors overboard on carrier Eisenhower; 2 rescued; several dozen missiles lost.
- 31 Oct. 12-foot swells on carrier Vinson, sailor swept overboard, lost.
- 1 Nov. Boiler room fire on oiler Monongahela, 9 suffer smoke inhalation.
- 9 Nov. A-7E Corsair 2 crashes into apartment complex in Smyrna GA; 2 killed, 4 injured.
- 11 Nov. Destroyer Kinkaid collides with merchant ship; 1 sailor killed, 5 injured.
- 11 Nov. Two A-6 attack bombers dropped bombs near a capsite; one injured.
- 14 Nov. Amphibious assault ship Inchon catches fire in Norfolk; 31 injured.
- 14 Nov. F-14 Tomcat fighter crashes at sea, FL training flight, no injuries.

(Source: San Francisco Chronicle, 15 November 1989, p. A4)

The Iowa gun explosion last summer was clearly not software related. Of the above items, the Lexington landing, the F-18 bombing of the USS Reeves, and the A-7E certainly involved computer controls, although there is no evidence implicating the computers. Erroneous human computer input is a possible cause of the Reeves bombing. Human error seems to account for the rest.

Artificial lightning

Lightning may be natural, or may actually be stimulated artificially by man-made conditions in situations in which lightning might otherwise not occur. The latter occurred in the second and third of the following cases:

... three spectacular lightning accidents involving aircraft or spacecraft: (i) In 1963, a Boeing 707 flying at 5000 feet near Elkton, Maryland, was struck and destroyed by lightning, killing all occupants (3). Lightning apparently burned through one of the metal wings, or in some other manner entered the fuel tank inside that wing, and caused the fuel vapor there to explode. (ii) In 1969, Apollo 12 artificially initiated (or "triggered") two lightning flashes, one to ground and one intracloud (IC) discharge, when it was launched through a weak cold front that was not producing natural lighting (4). Although this rocket-initiated lightning caused major system upsets and minor permanent damage, the vehicle and its crew survived and were able to complete their mission successfully. (iii) In 1987, an unmanned Atlas-Centaur vehicle (AC/67) was launched into weather conditions that were similar to those present at the launch of Apollo 12 and triggered a lightning discharge to ground (5). This discharge upset the computer memory in the vehicle guidance system and produced an unplanned yaw rotation, and the associated stresses caused the vehicle to break apart.

The preceding paragraph is excerpted from an article in the 27 October 1989 issue of *Science*, Natural and Artificially Initiated Lightning, by Martin A. Uman and E. Philip Krider, pp. 457-464. References 3-5 are given in the article.

The Atlas-Centaur case was previously reported in the ACM Software Engineering Notes (vol 12 no 3). The Apollo 12 case has not --to the best of my knowledge-- been noted here previously. More generally, the detailed discussion of artificially triggered lightning in the Science article should be particularly interesting to RISKS readers. PGN

Re: Apollo 12 (From Henry Spencer)

An interesting sidelight is *why* Apollo 12 survived the lightning strikes. The Apollo spacecraft's electronics got scrambled quite thoroughly, but the independent computers running the Saturn V booster were unaffected. They were in a much less exposed position, on top of the booster proper, underneath the Apollo spacecraft assembly. (They may also perhaps have been better protected against electrical upsets, although I don't know that for sure.)

Early in the Saturn program, there had been some discussion of the idea of saving weight by having the spacecraft computers run the booster as well; Wernher von Braun vetoed the idea and insisted on the booster having its own control system. This was probably more because of potential problems with changing payloads -- the Saturn V was meant to be NASA's heavy booster well into the 1980s, launching much more than just Apollo -- but I seem to recall that better protection for the electronics was mentioned as well.

Mariner I [once more] (From Mark Brader)

The new Usenetoid newsgroup alt.folklore.computers (a.f.c) has been having a discussion of the Mariner 1 space probe failure in 1962 due to a missing '-' (Arthur C. Clarke: "The most expensive hyphen in history." The vehicle cost $18,500,000.) which was discussed at length in RISKS in November and December 1987.

As was discussed in RISKS, a popular but apocryphal version of this story -- even appearing in computer textbooks -- is that a '.' was substituted for a ',' in a FORTRAN DO statement, converting it to an assignment. But no contemporary evidence was ever cited to support that story.

Now the a.f.c discussion began with exactly that apocryphal story; someone has posted the old Risks discussion to clean that up. But this time one thing is different. Someone else has posted giving a likely explanation of the FORTRAN DO version of the story. Notice, by the way, that it did not cost even one spacecraft, let alone the billion dollars claimed in one of the textbooks.

Fred Webb writes in alt.folklore.computers:

Subject: Fortran story - the real scoop Summary: I was there!

... This kind of thing is a common Fortran bug, so there are probably many different stories going around with a similar theme. Some of them are probably true. I do know of one such instance that really did happen, at Nasa.

I worked at Nasa during the summer of 1963. The group I was working in was doing preliminary work on the Mission Control Center computer systems and programs. My office mate had the job of testing out an orbit computation program which had been used during the Mercury flights. Running some test data with known answers through it, he was getting answers that were close, but not accurate enough. So, he started looking for numerical problems in the algorithm, checking to make sure his tests data was really correct, etc.

After a couple of weeks with no results, he came across a DO statement, in exactly the form ... indicated above. After changing the '.' to a ',' the program results were correct to the desired accuracy. Apparently, the program's answers had been "good enough" for the sub-orbital Mercury flights, so no one suspected a bug until they tried to get greater accuracy, in anticipation of later orbital and moon flights. As far as I know, this particular bug was never blamed for any actual failure of a space flight, but the other details here seem close enough that I'm sure this incident is the source of his version of the story.

[Sent to Risks by Mark Brader, SoftQuad Inc., Toronto. See RISKS-8.75 and *SEN* 14 5 for the missing 'bar' in 'R dot bar sub n' expression that contributed to the loss of Mariner I, with details provided by Paul Ceruzzi. So, after all these years of confusion, we can now believe that *both* stories are true, although the comma was not the bug that blew the mission. I hope this finally puts all the confusion to rest. PGN]

Congress repeals catastrophic insurance, SSA still collects premiums (From Rich Rosenbaum)

A story on "All Things Considered" (National Public Radio) on the evening of 5 Dec 89 reported that although Congress has recently repealed the catastrophic illness law, the Social Security Administration (SSA) will be unable to stop collecting insurance premiums until 3 June 1990. It seems that the SSA "warned" Congress that unless legislative action was taken by October 24, they would be unable to enact the changes quickly. "Apparently there are 150 different software programs that have to be changed and the computers just are not geared up to do that." Once again, the computer is at fault. Interestingly, it is possible for the SSA to raise the premium in January to $5.30. By the way, people will eventually get their money back, without interest.

SSA software maintenance (From Dan Franklin)

The news about the SSA being unable to reprogram its computers in time for the catastrophic health care bill repeal comes as no surprise to anyone who's read "Nations at Risk: the Impact of the Computer Revolution" by Ed Yourdon (1986, YOURDON Press):

"Indeed, the SSA problems are not unique, and are no reflection on the energy, talent or dedication of its staff -- but rather the accumulation of old hardware, old software, and a general lack of understanding on the part of Congress of the difficulties of dealing with massive volumes of data. For the SSA, massive means 446 billion [bytes] of disk storage to service 650,000 inquiries each day. It means 113 tons of computer printouts per month; 380 million wage reports per year, and 40 million checks per month. As former commissioner John A. Svahn says, only a "daily miracle" gets the monthly checks out on time. Having worked with the SSA computer people, I can personally testify to their enormous

energy and professionalism, and I firmly believe that the $478 million five-year modernization program approved by Congress in 1982 will eventually (though not in five years) get the organization back in control."

The demurral about the time needed has unfortunately now been vindicated. [How demurralizing! P.]

There's more on p. 432:

> "Calculating the cost-of-living increase for 50 million recipients of Social Security benefits takes 20,000 hours of computer time on older computer systems within the SSA. [That's 1.44 seconds per recipient!]
>
> "When the SSA upgraded its computer systems in 1981 from five-digit checks to six-digit checks, it required 20,000 man-hours of work and 2,500 hours of computer time to modify 600 separate computer programs.
>
> "The morale in the SSA maintenance group was so bad at one point that one of the programmers was caught urinating on a disk pack..."

"Before you laugh too loudly at this, remember that the SSA has one of the better MIS organizations in the country. They deal with gargantuan volumes of data, and they work in a political environment that defies imagination -- but they get the job done, and they get the checks out each month..."

True, an incorrect check is lots better than no check at all!

These passages are used to help illustrate one of the book's points, which is that large information systems all over the U.S. are suffering badly, and that problems with these systems are a significant factor keeping us from being more competitive. He makes a persuasive case; the book is worth reading (though redundant towards the end). Dan Franklin

Congressional report on Bugs in the System

There was extensive discussion in the on-line RISKS Forum on a report written by James H. Paul and Gregory C. Simon, "Bugs in the system: Problems in federal government computer software development and regulation" (Subcommittee on Investigations and Oversight of the House Committee on Science, Space, and Technology, Government Printing Office, Washington, D.C., September 1989). The report was also summarized by M. Mitchell Waldrop in the AAAS weekly, Science, 10 November 1989, vol. 246, p.753. The report takes to task the waterfall model, the system and software procurement process. "Software is now the choke point in large systems." "Government policies on everything from budgeting to intellectual property rights have congealed over time in a manner almost perfectly designed to thwart the development of quality software." Paul told Science, "The federal procurement system is like a software system with bugs." James Paul spent 2 years and a lot of effort talking to many people, and the report is quite impressive. Let's hope it does some good.

Army shuts down computers and goes home due to rain (From Rodney Hoffman)

Roddy Stinson is a columnist for the San Antonio, Texas "Express-News". Here's one Question & Answer from his column of 14 Nov 1989 under the headline 'Rainstorms Didn't Stop the Army When I Was In It':

The complaint desk is open --

Plaint: I am a retired Army sergeant. My wife just got out of intensive care at Brooke Army Medical Center. I tried to call BAMC to make a medical appointment for her, and this is the message I got: 'The patient appointment system cannot operate at this time. Due to inclement weather, the computers had to be taken down. Please continue calling periodically. Thank you. This is a recording.' That's pitiful. That's ridiculous. What happened to typewriters and phones? If a rainstorm can shut down the country, we're in big trouble. I'll tell you one thing -- rainstorms didn't stop the Army when I was in it. They told me to keep marching, and I did.

[Stinson:] A spokesman for BAMC explained: "This (computer shutdown) happens every time there is a possibility of thunderstorms because the central appointments system is linked to a mainframe a mile and a half away, and if lightning hits the lines, everything on there could be erased." When I expressed skepticism, he added: "Believe me, it has happened. Lightning takes out our phone system and electricity on a regular basis." Progress marches on.

Pentagon Computer Costs (From Gary Chapman)

The New York Times issue of 1 Dec 1989 features a story by Jeff Gerth that says that the modernization of a Pentagon computer system used for general data processing is a billion dollars over budget, and far behind schedule. And the congressional report released about this system says that Pentagon computer systems have experienced "runaway costs and years of schedule delays while providing little capability."

Charles A. Bowsher, the head of the General Accounting Office, says that problems with the Pentagon's accounting system may impede efforts to reduce spending in the Department of Defense because of inaccuracies in the data used to manage the Department.

Today's New York Times article reports only on cost overruns and delays in accounting and data-processing systems used by the Department of Defense and the services. But there are also these examples one could add to the list:

• The C-17 cargo plane being built by Douglas Aircraft has a $500 million cost overrun because of problems in its avionics software, and the software contractor has been fired, according to a member of Congress.

• The B-1 bomber still needs more than $1 billion to improve its ineffective air defense software. The B-1 was originally sold as a "penetrating bomber," meaning it was supposed to be able to penetrate Soviet air defenses. Because of problems with its computer software, however, the B-1 is not expected to be able to penetrate Soviet air space, and that's why the Air Force is asking for the B-2 (which has its own software problems). (At one point the B-1 electronic countermeasures software created what was called a "beacon" effect, meaning it would actually alert Soviet air defenses and give their radars a clearer signal of the aircraft than they would have if the airplane's systems had been turned off.)

• The software for the modernization of the Satellite Tracking Control Facility is about seven years behind schedule, about $300 million over budget, and will provide less capability than what the original contract called for.

• The modernization of the software at NORAD headquarters is about $250 million over budget, years late, and still non-operational.

• The Airborne Self-Protection Jammer (ASJP), which is an electronic air defense system installed in over 2,000 Navy fighters and attack planes, is $1 billion over budget, four years behind schedule, and, according to a Navy report, is only "marginally operationally effective and marginally operationally suitable."

As General Bernard Randolph, commander of the Air Force Systems Command, said in February, "We have perfect record on software schedules--we have never made one yet and we are always making excuses." Gary Chapman, Executive Director, CPSR

GAO Says IS technology is transforming the Government (From Dave Davis)

The Washington Post, 21 Dec 89 reports on a General Accounting Office study, "Financial Integrity Act" about Information Technology applications within the government. The overall message is that information systems technology is costly and risky. Here are some quotes:

"Federal agencies operate over 53,000 unclassified automated systems...life cycle costs in the billions of dollars..." The article reports costs of $17 billion for fiscal 89 versus $9 billion in fiscal 82 for these computer applications.

"Invariably these systems do not work as planned, have cost overruns in the millions and even hundreds of millions of dollars, and are not developed on time. Congressional interest... has increased..."

Some specific examples are cited.

"...defense [business as well as command and control] far exceeded their original costs estimates...fell significantly short of expectations...design flaws, misjudgments in requirements, poor program management."

The article describes a Navy financial system whose costs grew from $33 million to $479 over nine years of development. Also, an IRS system is estimated to cost $1 billion, and has not shown benefits from currently operational components.

Except for specific details, all of this is old news to many of us who have been involved in large systems of various kinds for a while. What does seem to be new are trends toward larger fiascos and for increased government concern a by people who control purse strings. Also, do stories of such failures indicate that we reach an intellectual brisk wall when we try to develop large systems? Or, are we simply repeating dumb mistakes? David Davis, MITRE Corp., McLean, VA

Air Force Radar Risk (update) (From Henry Cox)

Radar at U.S. Base Can Trigger Planes' Ejection Seats: Letter
From the Montreal Gazette, 23 November 1989, Knight-Ridder Newspapers

Robins Air Force Base, Ga. - The US air force has learned that radiation from its PAVE PAWS radar at Robins AFB could activate internal equipment - including ejection seats and fire extinguishers - on virtually all planes that land at the base. The disclosure was made in an Air Force "update" letter to Senator Sam Null (D-Ga.) made public this week by the

senator's Washington office.

Although the air force originally said that PAVE PAWS would not endanger electro-explosive devices other than those on the outside of its plane, a recent review of the radar has concluded otherwise, the air force letter said. "As a result, Air Force Space Command is co-ordinating with the Air Logistics Center at Robins AFB to implement procedures to ensure aircraft with internal EEDs are also protected," wrote Maj.-Gen. Burton R. Moore, the air force's director of legislative liaison. But Nunn, in a written reply to Moore dated Nov. 20, says that the air force hasn't fully answered his questions of last January, and has "raised new questions" with its latest update. "It would be helpful to know more about the hazard to such devices, what the devices are used for, and what aircraft are equipped with them. I would also like to know how the air force determined that these devices were at risk," said the Senate Armed Services Committee chairman in his two-page letter.

The radiation hazard to internal EEDs is the latest safety revelation concerning the southeastern PAVE PAWS - built too close the runway at Robins AFB. The radar, one of four nationwide, is designed to warn of sea launched missile attacks and track satellites in space. But since November of 1987, the air force has been turning off the north face Robins PAVE PAWS to protect vulnerable planes landing on its runway 3 kilometres north of the radar. According to air force documents obtained by Knight-Ridder Newspapers recently under the Freedom of Information Act, one aircraft at risk to PAVE PAWS is the Strategic Air Command's KC-135R tanker, some of which are based at the 19th Air Refuelling Wing at Robins. EED equipment on other aircraft includes "flare/chaff dispensers, pylon/ejector racks, tactical missiles, cruise missiles, crew escape, and engine start cartridges," according to air force documents.

[This problem was noted in *SEN* 14 2. The details are new. PGN]

Another runaway military computing project: WWMCCS (From Jon Jacky)

RISKS has carried occasional articles about problems with the WorldWide Military Command and Control System (WWMCCS). A history of the project since the early 1970's appears in the article, 'The Pentagon's Botched Mission', by Willie Schatz, *Datamation*, 1 Sept 1989, pp. 22-26.

From the lead paragraph:

"Seven years after the [WWMCCS modernization] project started, the military has spent $395.4 million, the users are outraged, the system is unfinished, responsibility for the project has been transferred, its name has been changed twice, and no one is entirely sure what will happen now."

(From Tom Reid)

I worked with WWMCCS in 1985/6 and many of their problems stemmed from a technology bet that they had made 3-4 years earlier. They had a software first philosophy that stressed using as much commercial-off-the-shelf (COTS) software as possible. They bet that by 1986, respondents to the RFP would be able to bid COTS 1) multi-level secure operating systems and 2) distributed heterogeneous DBMSs. It is 1989 and there are still precious few (if any) examples of either. When it became obvious that neither was going to appear by 1985/6 when they were scheduled publish the RFP, they were not prepared and the program began scrambling to find stop gaps. It was downhill from there.

Selling Government-Held Information (From Peter Jones)

On CBC's Daybreak program on 6 December 1989, there was an interview about the possibility of selling information held by government institutions to private companies. For example, names and addresses of municipal bondholders or property owners could be used for direct mailing.

Currently, there is a dispute concerning the information held by the Inspector of Companies on company names, and names and addresses of directors. This information, although publicly available, is regarded by the Inspector as confidential. For example, it would be possible to guess a person's political affiliations from the presence of his name on the board of directors of a political organization.

There are two issues here, being disputed by the private companies on one side, and the government and the Quebec Civil Liberties Association on the other:

1) Prevention of access to confidential data. (A straightforward computer problem).

2) Making data available in a form that allows massive searching and matching.

This raises the privacy issues currently being disputed.