Risks to the Public in Computers and Related Systems

Peter G. Neumann plus contributors as indicated
SRI International EL-243,
333 Ravenswood Ave.,
Menlo Park CA 94025-3493
(1-415-859-2375; neumann@csl.sri.com)

Edited by Peter G. Neumann (Risks Forum Moderator and Chairman of the ACM Committee on Computers and Public Policy), plus personal contributions by others, as indicated. Opinions expressed are individual rather than organizational, and all of the usual disclaimers apply. To economize on space despite the enormously increasing volume of cases, we tersify many items and include on-line pointers to other items in the on-line Risks Forum, where (S i j:p) denotes *SEN* vol i no j page p (1997 = volume 22), and (R i j) denotes RISKS vol i number j. The RISKS archives are available on ftp.sri.com, cd risks. *SEN* archives are summarized at ftp://ftp.CSL.sri.com/illustrative.PS. Please send RISKS-related items to risks@CSL.sri.com. Read RISKS as a newsgroup (comp.risks), or subscribe via the automated listserv at risks-request@CSL.sri.com. Peter G. Neumann, SRI International EL-243, 333 Ravenswood Ave., Menlo Park CA 94025-3493 (1-415-859-2375; neumann@csl.sri.com).

Difficulties in developing large systems: IRS, etc. (PGN)

The IRS is apparently going abandon its Tax Systems Modernization effort, on which it has spent $4 billion. In testimony for the National Commission on Restructuring ["reinventing"] the IRS, IRS Assistant Commissioner Arthur Gross (who less than a year ago took on responsibility for IRS computers) stated that the systems "do not work in the real world." (Past criticism has come from the Government Accounting Office and the National Research Council. See also RISKS-17.96, 18.23-25, 18.43.) Gross noted that the IRS lacks the "intellectual capital" for carrying out the effort. One system had been cancelled earlier (the program for converting paper returns to electronic form), and 12 more systems are under review. Gross is proposing to contract out the processing of individual returns to commercial firms (which raises all sorts of privacy issues), although that is only a small portion of the processing demands. [Source: An item from *The New York Times*, seen in the *San Francisco Chronicle*, 31 Jan 1997, A1.]

A subsequent editorial on the IRS's plight [*San Francisco Chronicle*, 2 Feb 1997] also reminds us that the FBI "threw away" a $500-million fingerprint-on-demand computer system and its crime information database, the State of California spent $1 billion on its nonfunctional welfare database system, along with more millions on BART and the DMV. Readers of RISKS are well aware of the difficulties of developing large systems (e.g., the next item). The real question is whether anyone is learning from the past experience.

California child-support deadbeat database flawed (PGN)

California has already spent $300 million on its Statewide Automated Child Support System (SACSS). The projected costs have escalated from the 1991 estimate of $99M. The Assembly Information Technology Committee, chaired by Elaine Alquist (D-SantaClara) has just issued a report suggesting that the system may have to be scrapped: "Due to significant problems in the SACSS application, many of which could go undetected until the project is fully implemented, it is unclear whether the project will ever fulfill the mandate of the federal government or the child support enforcement needs of California's 58 counties." [Source: *San Francisco Chronicle*, 2 May 1997, A22] The federal government is paying 90% of the development costs. If that funding were cut off, would they be accused of being a Deadbeat? (We might hear Grateful DeadBeat Dads singing.)

Alberta Stock Exchange shuts down again (Mich Kabay)

Angela Barnes and Brent Chang of the *Globe and Mail* (12 Mar 1997, B1) reported that for the second time in six sessions and the third time in 1997, "the Alberta Stock Exchange lost a day of trading because of problems with its leading-edge computerized trading system."

- System failure occurred at opening of trading on 11 Mar 1997 at 07:30 MST.
- Technicians worked until 13:00 and tried to restart software, but programs failed immediately.
- Bug fixes continued all night.
- Previous software errors stopped trading on the ASE for an entire day on 4 March and during January; two other day-long halts occurred in 1996 after the software went online in May.
- Brokers depend on the software to trade through modem links from their offices.
- The trading floor is supposed to be closed permanently by 21 March 1997.
- Consequences of the breakdowns include lost commissions, lost business opportunities, and loss of confidence in the ASE.
- EFA Software Services of Calgary responsible for trading software for other exchanges around the world, including the Palestine Securities Exchange.

Internet routing black hole (PGN)

On 23 Apr 1997 at 11:14a.m. EDT, Internet service providers lost contact with nearly all of the U.S. Internet backbone operators. As a result, much of the Internet was disconnected, some parts for 20 minutes, some for up to 3 hours. The problem was attributed to MAI Network Services in McLean, Virginia (www.mai.net), which provided Sprint and other backbone providers with incorrect routing tables, the result of which was that MAI was flooded with traffic. In addition, the InterNIC directory incorrectly listed FL Internet Exchange as the owner of the routing tables. A "technical bug" was also blamed for causing one of MAI's Bay Networks routers not to detect the erroneous data. Furthermore, the routing tables

Sprint received were designated as optimal, which gave them higher credibility than otherwise. Something like 50,000 routing addresses all pointed to MAI [Missing in Action on the Internet?]. [Source: Inter@ctive Week Online, 25 Apr 1997, article by Randy Barrett, Steven Vonder Haar, and Randy Whitestone.]

Once again we suffer from inadvertigo, illustrating how the effects of a seemingly small inadvertence and other collateral factors can cause widely propagating problems.

Playboy strikes again (PGN)

TCI's cable-TV provider in Springfield, Missouri, was testing its planned inclusion of the Playboy Channel (to begin in Feb 1997), when the Cartoon Network Channel suddenly began airing the Playboy video along with the regularly programmed Flintstones' audio. The results were perhaps more noticeable than they might have been, because bad weather had closed the local schools and children were at home. [Source: Associated Press item in the *San Francisco Chronicle,* 17 Jan 1997, AS2.]

There seems to be something magnetically RISKS-attractive about the Playboy Channel, which in summer 1996 appeared unscrambled in the Palo Alto area because of a power-failure-induced chip failure (RISKS-18.50). A PC program [a nicely overloaded acronym, since the program was presumably not politically correct!] had previously appeared in the *Jeopardy* time-slot in the Chicago area for 10 minutes, due to a screwup (RISKS-18.22). Of course, what comes around goes around; 10 years ago the Playboy Channel was intentionally disrupted by a CBN employee, with satellite-spoofed programming declaiming "Repent Your Sins" (RISKS-10.62).

Computer threatens 11,000 car owners in Finland (Toomas Tamm)

In the Finnish TV news on 9 Jan 1997, it was reported that the Finnish car registry had sent mail to 11 thousand car-owners stating that the registration of their cars would be dropped from the registry, "because the car has been out of use." The registry representative said this was caused by a "computer error" the exact cause of which is being investigated. The registry then sent out 11,000 apology letters.

Computer glitch gives investors instant loss of balance at Schwab (Norm deCarteret)

A program error caused Schwab's computers to omit a significant number of mutual funds when investors used Telebroker to track holdings by phone, leading some of them to believe themselves broke. The problem existed from Monday afternoon through late Tuesday evening scaring scores of investors. Janus, Putnam and Schwab's own funds were among those omitted from net asset calculations.

Tracey Gordon, Schwab spokeswoman: "We were making some system changes when there was a program error." On why the problem went on so long: "Mutual funds are priced once a day. We found that it would be cleaner and simpler to wait until the next regularly scheduled market change to update the system." Cleaner and simpler for Schwab, presumably. Gordon said investors who made panicky trades as a result "would be made whole" but there'd be risks in determining both the who and the how much.

NASD loses records on 20,000 brokers (Stern)

The National Association of Securities Dealers (NASD) is the self-regulatory organization that oversees broker-dealers and their employees in the United States. It maintains a database of brokers and any disciplinary actions taken against them. The database can be accessed by calling Disclosure, Inc. (1-800-638-8241 in the U.S.) Before doing business with a new broker-dealer or a new broker, it's a good idea to call Disclosure to check if they have been a problem for other investors in the past. Unfortunately, the NASD has purged 20,000 records from their files. According to the Associated Press, "The NASD said it inadvertently issued faulty guidelines telling clerks that "revised" rules allowed them to purge a broad range of disciplinary data from the central registration depository."

The risks are (at least) threefold. First, that investors will not have access to this valuable information and that people may deal with unscrupulous brokers as a result. Second, other regulatory agencies that rely upon the NASD's record will not be able to perform their functions. Thirdly, the NASD itself will not be able to refer to past disciplinary records on these brokers in deciding penalties in response to new complaints. The NASD believes it will be able to reconstruct its records in a couple of months. [Can you spell *backup*?]

Telstar 401 catastrophic failure (Lauren Weinstein)

On Saturday morning, 11 Jan 1997, AT&T's Telstar 401 satellite, with a full complement of both C and Ku band transponders, went dead. Technicians were unable to reestablish contact. The satellite normally carries both broadcast network and syndicated television programming. The networks, as "platinum" customers, were quickly switched to an alternative bird. Almost everyone else has been scrambling to find transponder space for their programming. The risk? Don't assume that a satellite will always be there! (Lauren, Moderator, PRIVACY Forum www.vortex.com)

Five-million-dollar bug (David Kennedy)

A big brown cockroach crawls across the table in the laboratory of Japan's most prestigious university. The researcher eyes it nervously, but he doesn't go for the bug spray. He grabs the remote. This is no ordinary under-the-refrigerator-type bug. This roach has been surgically implanted with a micro-robotic backpack that allows researchers to control its movements. This is Robo-roach. ... Professor Isao Shimoyama, head of the bio-robot research team at Tokyo University says, electronically controlled insects carrying minicameras or other sensory devices could be used for a variety of sensitive missions – like crawling through earthquake rubble to search for victims, or slipping under doors on espionage surveillance. ... The controls, however, still have a few serious bugs of their own.

Swiss researcher Raphael Holzer, part of the Tokyo University team Holzer jolts a roach with an electric pulse to make it move slightly to the right and keep to an inch-wide path. Instead, the roach races off the edge of a table into Holzer's outstretched hands. "The placement of the electrodes is still very inexact," he admits, setting the bug back on track. ... Holzer is optimistic. "The technology isn't so difficult," he said. "The difficulty is to really understand what is happening in the nervous system." [Electronic Roach Implants Probed, By Eric Talmadge, Courtesy of Associated Press via America Online's News Profiles]

Redundant virtual circuits lead to single point of failure (Sidney Markowitz)

This note from Finland was passed on to me by a friend. It points out the Risks of working with virtual systems while carrying assumptions and habits from the real (physical) world. "We had a data line breakdown last week, and no Internet connections worked. It happened that there was heavy icing on the line between Oulu and Kajaani, which caused the break. We had a reserve line, but that was also broken. That line was leased from Finnet, and it happened that as logically separate it was physically that same line that Finnet had leased from the primary operator! The agreement with Finnet was ended immediately."

[For newer readers, we recall New England being cut off from the rest of the ARPAnet by a single cable cut knocking out 7 links on 12 Dec 1986 (S 12 1; R 4 30), and the Annandale VA incident on 14 Jun 1991 that took out two separate fiber cables (S 16 3; R 11 92). PGN]

Southwestern Bell cannot handle the "@" sign (Mark Brader)

A *Houston Chronicle* article by Dwight Silverman was forwarded to comp.dcom.telecom by Tad Cook about various changes that Southwestern Bell is planning to make in their directories. One of the changes is that they plan to list e-mail and WWW addresses for businesses that want to supply them. However, this will not be possible for residential listings at first, because (I swear, this is just how the posting appeared): "Right now we have a certain system constraint in our residential listings database that prevents us from printing certain characters on a page," Hillyer said. "The biggest problem is that we can't print the sign." The sign is a crucial part of all e-mail addresses, separating the user's name from the computer system – or domain – he uses." ["@" is not commercial enough?] ("But I do't have a '' key o my termial." – Ly[nn] Gold)

Electronic airline ticketing (Robin Burke)

I have had recent and vivid evidence of the risks of much-hyped "electronic ticketing" systems for air travel. My wife called to confirm her reservation on a return flight, only to discover that, according to the airline she had already flown a week earlier. "You've used that ticket," she was told. Since electronic ticketing procedures require that the agent match the user's ID with the ticket information, she was treated like someone trying to scam the airline by flying twice. Fortunately, the date of usage was different than the date for which the ticket was issued, although the flight number was the same, and she had various records, such as her credit-card receipts, through which to assert her identity, but only after many hours on the phone.

The supervisor who finally resolved her case seems to be handling a lot of electronic ticketing problems. The agent is supposed to look at the passenger's ID, and pull up the ticket record corresponding to that traveler. However, there is also a receipt for the electronic ticket: "not valid for travel" that has the name and ticket number on it. Apparently, in this case, the gate agent used the ticket number from the receipt, but typed it in wrong, then failed to notice that the ticket record retrieved was for a different passenger than the one named on the receipt. No record is made of the validating transaction (the agent matching the ID against the ticket record), except for the agent marking the record as used, so the airline has no way of knowing who actually traveled on our ticket, and we had no way, within the system, of documenting the fact that the ticket had been used by someone else. I, for one, will stick with a physical ticket.

Shetland Times copyright suit (Brian Randell)

The Times (London), 21 Jan 1997, carries a report of the court case concerning whether the use of headlines taken from the *Shetland Times'* Website, as links back to the stories at that site, was a breach of copyright. (See S 22 2:20 and R 18 64,78,79,81.) "The inclusion of the headlines of one newspaper in the Internet Website of another newspaper was, prima facie, infringement of the copyright belonging to the original newspaper. Lord Hamilton, sitting in the Outer House of the Court of Session, so held, granting interim interdict in an action of declarator of infringement of copyright and interdict at the instance of *Shetland Times Ltd* against Dr Jonathan Wills and another."

This was under Scottish Law, and I'm not sure what an "interim interdict" is, but it sounds painful for the people who were doing the copying. However it would seem that the judge was sympathetic to *The Shetland Times* because: "A caller gaining access to the defendants' Website might, by clicking on one of those headlines appearing on the defenders' front page, gain access to the text as published and reproduced by the pursuers. Such access was gained without the caller requiring at any stage to gain access to the pursuers' front page. Thus access to the pursuers' items could be obtained by bypassing the pursuers' front page and accordingly missing any advertising material which might appear on it."

What isn't clear to me from the article is whether it would be a breach of copyright to link to the articles without using the exact text of the headlines. [Follow-up discussion in (R 18 79,81).]

The (f)e-mail of the PCs is more deadly than the bail* (PGN)

The case involving Adelyn Lee and Oracle's CEO Larry Ellison (see RISKS-18.07-08) resulted in Ms. Lee being found guilty of perjury and falsification of evidence. She had previously won a $100,000 settlement against Oracle, using as evidence an e-mail message ("I have terminated Adelyn per your request.") supposedly sent to Ellison by her former boss, Oracle VP Craig Ramsey. The prosecutor claimed that Lee had sent the message herself from Ramsey's account. She faces up to four years in jail. Subsequently, the judge ruled that she may not use any of that settlement money to pay her bail. [Source: *San Francisco Chronicle,* 29 Jan 1997, A11, and 31 Jan 1997, E1]

[This is another case involving the credibility of digital evidence in penetrable, tamperable, and spoofable environments. *The boldface title line is drawn from a well-known poem. PGN]

E-mail saboteurs interfere with Columbian kidnapping negotiations (Miranda Mowbray)

In August 1996, sixty Colombian soldiers were kidnapped by the Fuerzas Armadas Revolucionarias de Colombia (FARC), a Marxist-Leninist guerrilla group. The Colombian Government announced in early 1997 that they would change from negotiating with the kidnappers through face-to-face meetings with intermediaries (which is slow and dangerous) to negotiating by e-mail. Just after the announcement, the Government received a puzzled message from the FARC, saying that they had already received two e-mail messages claiming to be from the Government. Those messages apparently were spoofs created by right-wing saboteurs who do not want any negotiations to take place. [Source: BBC World Service News, 2 Feb 1997]

Will-o'-the-w-ISP! More on AOL (PGN)

1. AOL was inaccessible to new sign-ons for about 20 minutes on 2 Dec 1996, due to a "software system bug" in preparing for the influx of users expected when the flat-rate charges went into effect; the 165,000 existing sign-ons were left intact. After fixing the bug at 4:55pm, AOL then blocked about one of every 10 sign-on attempts for the evening. (We note this case retrospectively for the RISKS archives, although it may seem insignificant in light of more recent problems.) [*The Washington Post,* 3 Dec 1996, C3.]

2. AOL's network bombed again, beginning at 2pm on 5 Feb 1997, and was not fully restored until about 4:30pm. The problem was attributed to a "technical glitch" in a software upgrade. [*San Francisco Chronicle*, 6 Feb 1997 (R 18 81). When have we heard that one before?]

3. Subsequently, AOL users were prompted to log off after 45 minutes, and bounced ten minutes later if they had not complied. However, certain games mask the dialog box, so that users would not see the warning message. (R 18 81).

4. More extensive AOL e-mail outages were required in early April 1997, when service was suspended for several days in order to do an upgrade (R 19 07).

Cyber Promotions: spam and get spammed (PGN)

1. Cyber Promotions Inc. (one of the largest conduits for junk e-mail) was barred on 3 Feb 1997 by a federal court from sending unsolicited e-mail ads to CompuServe's 5 million subscribers. The next day, a different federal court barred them from falsifying their FROM: addresses. [I presume CPI will still find ways to go through the (pro)motions.] [*San Francisco Chronicle* squib, 6 Feb 1997.]

2. Cyber Promotions was hit with a temporary federal court restraining order in response to Earthlink's complaint against their electronic "trespassing". They also agreed to pay CompuServe $65,000 to settle a federal lawsuit, and agreed to stop spamming CompuServe users. (They had earlier agreed to a similar settlement with AOL.) Also, in the same two-day period, they experienced a 20-hour retaliatory reverse-spam that flooded their computer system with millions of requests for hardware identification numbers [which some might call a taste of their own medicine]. That attack was stopped by filtering out 50 net addresses. [Source: an AP item by Jennifer Brown, seen in the *San Francisco Chronicle,* 9 May 1997, C2; R 19 13]

F-16 incidents involving TCAS (PGN)

There have now been four recent incidents involving F-16s and commercial airliners with the TCAS automated collision avoidance system.

1. On 5 Feb 1997, two Air Force F-16s closed on a Nation's Air Boeing 727 passenger jet heading for JFK in NY. A TCAS alarm caused the 727 pilot to take evasive action, flooring three passengers and crew members. This occurred in a fairly large restricted area through which the 727 had been cleared to fly. One of the F-16 pilots had earlier identified the 727 as a passenger plane, but continued to chase it "as an intruder into his airspace". The instructor pilot told his trainee pilot to stay out of the way "till this, uh, bozo gets out of the airspace." He was eventually ordered to stop the chase, but "the command may have been delayed because the fighter pilot was on the wrong frequency" (according to the Air Force report).
2. On 7 Feb 1997, four Air National Guard F-16s from Andrews Air Force Base passed an American Eagle commuter plane bound from Raleigh to NY. Three of the F-16s were above the commuter plane, one below. A TCAS alarm caused the American Eagle pilot to take evasive action.
3. Also on 7 Feb 1997, two Air Force F-16s entered the safety zone around an American Airlines jet over Palacios TX.
4. Also on 7 Feb 1997, two Air Force F-16s entered the safety zone around an Northwest Airlines jet over Clovis, NM.

The Air Force insists that none of these cases was a close call (that is, with less than 500 feet separation), and that such close encounters have happened routinely in the past without causing concern – before the advent of TCAS. So, we can chalk this up either as an indication that TCAS works (albeit too well?), or as a failure of the Air Force to understand the risks of false alarms in someone else's safety system!

[Sources: items in *The Washington Post,* 8 Feb 1997, *Los Angeles Times,* 11 Feb 1997, A14, and *The New York Times,* 19 Feb 1997.]

B777 autopilot/flight-director problems? (Peter Ladkin)

Flight International (19-25 Feb 97, p4) reports that the UK AAIB is looking into an uncommanded-rudder-movement incident on a British Airways Boeing 777-200A in October 1996. The B777 is a fly-by-wire (FBW) aircraft. The aircraft departed Heathrow en route Jeddah, and was forced to turn back. A UK CAA Occurrence Report talks of uncommanded movement of rudder and rudder pedals during climb and cruise, at random intervals. The flaperons were also observed to move, it is surmised in counterresponse to the rudder movements. "Large rudder input" was required on the landing. An intermittent fault in the two autopilot/flight-director computers is suspected, and they're being lab-tested – as are the rudder backdrive actuators.

A320 flight-control Anomalies. Peter Ladkin contributed a very informative article on A320 flight-control computer anomalies (R 18 78).

Suit over computer use (David Kennedy)

The University of Wisconsin-Madison is facing a sexual harassment lawsuit that claims a former medical professor used campus computers to copy hundreds of pornographic pictures from the Internet. (Another employee is suing because the professor propositioned her.) [Source: UW prof accused of copying porno pics, UPI US & World, 13 Feb 1997, Courtesy of United Press International via CompuServe's Executive News Service]

[Privacy fanatics balk when companies claim privilege over the contents and uses of the systems the companies own. In this case, the university is being held responsible for the actions of one of their employees. Given the academic-freedom environments in most (all?) American Universities (and probably elsewhere), the university is in a no-win position. DMK]

Bank sued for racist e-mail (David Kennedy)

Two black employees of the Citibank NA unit of Citicorp filed a race discrimination lawsuit after racist jokes were allegedly sent via e-mail by several bank supervisors at the end of Jan 1997. The e-mail was identical to a set of racially charged jokes at the center of a lawsuit against Morgan Stanley & Co. The plaintiffs, Alvin Williamson, a vice-president, and Brenda Curtis, a secretary, contend that several Citibank supervisors, including vice-presidents, spread the offensive e-mail to specific colleagues around the country. The e-mail created a "pervasively abusive racially hostile work environment," the plaintiffs said in their lawsuit. [The suit claims little or no action was taken against those who spread the message, although the company acknowledged an incident did take place and it was "putting into effect disciplinary actions" against the perpetrators. Another company is being sued for objectionable content of employee computer use. DMK. Source: Citibank Workers File Bias Lawsuit Over Racist E-Mail, by Frances A. McMorris, WSJ reporter (Dow Jones, 18 Feb 1997), Courtesy of the Dow Jones News Service via CompuServe's Executive News Service]

Computer glitch triggers mailing of multiple driver's licenses (Dave Tarabar)

The Boston Globe, 20 Feb 1997, has a picture of a woman holding six copies of her new driver's license which came in the mail on the same day.

Two years ago, the Massachusetts Registry of Motor Vehicles converted to a new state-of-the-art system for producing driver's licenses. When a person renews a license, a digital color picture is taken. You are given a temporary paper license and are told that your permanent license will arrive shortly in the mail. The permanent license is a single piece of plastic (like a credit card). It should be more tamper-resistant than previous licenses, which had a Polaroid picture laminated to paper. However, in certain cases, the system was spitting out multiple copies of a license and mailing them on the same day. A spokesman for the Registry says that a computer programming error has been identified and fixed. The Registry says that about 50 people reported receiving multiple licenses. The major risk here is that extra licenses could be sold (or stolen) for the purpose of false IDs [although that would open the seller up to identity theft! PGN]

Another MacInTax glitch (David Kennedy)

At the beginning of March 1997, Intuit Inc. sent a letter to its MacInTax users detailing a potential pitfall for electronic filers. Users who fail to save their documents before filing them electronically may receive word from the IRS of an incomplete filing. The company said the problem will likely affect only a small percentage of users, as most would opt to save their work before transmitting files. However, there are some customers who tend to go straight to the electronic filing function without saving. [Patch at http://www.intuit.com/ or by disk.] In a statement, Intuit Vice President adequate fail-safe systems.

Leap-Year software bug gives 'million-dollar glitch' (Jim Towler)

Too many folks are suggesting that new programs are all OK and it's only the "old mainframe stuff" that will have problems with Year 2000. Well, people are still writing code with bugged date logic.

A computer glitch at the New Zealand Aluminium Smelter plant at Tiwai Point in New Zealand (South Island) at midnight on New Year's Eve 1996 left a repair bill of more than NZ$1 million. Production in all the smelting potlines ground to a halt at midnight, when the computers unexpectedly all shut down. General manager David Brewer said the failure was traced to a faulty computer software program that failed to account for 1996 being a leap year: the computer was not programmed to handle the 366th day of the year. The same problem occurred two hours later at Comalco's Bell Bay smelter, in Tasmania, Australia. (New Zealand is two hours ahead of Tasmania.) Both smelters use the same program,

which was written by Comalco computer staff. Before the Tiwai problem could be fixed that afternoon, five cells had over-heated and were damaged beyond repair. Mr. Brewer estimated the replacement cost at more than NZ$1 million. [Source: (*The Dominion* – Wellington, New Zealand, 8 Jan 1997) via NZPA [New Zealand Press Assoc.]

Apollo date bug coming soon: 2 Nov 1997 (Jim Rees)

Year 2000 is coming earlier for users of Apollo workstations. At 14:59 GMT on 2 Nov 1997, the high bit of the Domain/OS system clock will become set, and system bugs will prevent machines running unpatched software from booting. HP has released a fix, but it only runs on newer equipment, and has a bug of its own. Users of Apollo machines built before the dn3000 will simply be out of luck. (Details are available at http://pisa.citi.umich.edu/date-bug .)

1997 APRIL FOOLS' ITEMS:

• French immune to Y2K: quatre vingts dix neuf (4x20+10+9) will increment to cinq vingts (5x20); Windows ninety-ten will adopt similar strategy (R 19 01)

• Proposal to lengthen the second by 0.00001312449483 to eliminate leap years (R 19 01) or slow down the earth's orbit accordingly (R 19 02)

• Microsoft buys Sun in order to kill Unix (R 19 01)

• Hale-Bopp solar wind (cosmic radiation) causes ticking and buzzing in computer mouse; problem worsened by Internet acting as giant antenna (R 19 02)

OTHER ONE-LINERS:

• 2 jets in near-miss approaching LAX; Brazilian VASP MD-11 pilot blames autopilot, others blame pilot (R 19 10)

• 747 tail scrapes runway; center of gravity miscalculated by improper program upgrade (R 19 11)

• Minireview of James Sander's *The Downing of TWA Flight 800* (R 19 12)

• Risks in IVHS automated vehicles (R 19 08,10,11)

• U.S. Social Security Admin systems cannot handle nonAnglo names, affecting $234 billion for 100,000 people, some back to 1937 (R 18 80)

• Paper-clip causes hard-drive overflow, triggering traffic-control computer failure stopping trains in south Finland for an hour (R 19 10)

• Bre-X Minerals gold scam (Indonesian no-gold) causes unprecendented trading, crashing Toronto Stock Exchange computer system (R 19 09); Bre-X, stock from $200 to .06, filed for bankruptcy (news item, 9 May 1997)

• "My Hairiest Bug War Stories" (*Communications of the ACM,* April 1997, pp. 30-37) on debugging, including a program that worked correctly only on Wednesday, because the overwritten 9th byte was supposed to contain a 'y'! (R 19 09); more examples in (R 19 10,11)

• Bremen hospital computer uses financial bottom-line whether to give intensive care; local government objects (R 18 84)

• Damages awarded after Sleepezee Beautyrest high-tech bed controls went berserk. Electromagnetic interference? (R 19 11)

• "Heading off emergencies in large electric grids" (*IEEE Spectrum* article, April 1997, pp.43-47) (R 19 09)

• Limitations of mouse-based interfaces on disabled persons (R 18 87,88)

• Mail-merge program generates 12,000 amendments for Ontario legislature in blocking attempt (R 19 06,08,09)

• Ariane 5: simple formal approach would have detected flaw? (R 18 89-91)

• Controversy surrounding *Dallas Morning News* posting news of alleged Timothy McVeigh "confession" on their Website. Item obtained via computer breakin? Early Web posting to stave off injunction? (R 18 85) Bogus memo allegedly planted in attempt to trap a witness?

• Erroneous Skytel paging network broadcast mushrooms, deluges 100,000 customers, some of whom received 300 calls an hour (R 18 75)

• NY City electronic voting machines still lagging after spending $20M (R 19 06)

• Risks of IRS outsourcing processing of tax returns (R 18 81,82,87)

• More risks of allegedly random numbers: spoofability (R 18 89)

• Deep Blue in Deep Foo in first Kasparov match; chess board position A3 interpreted as command '3', necessitating reboot and loss of 20 minutes (transcript in R 18 78); Deep Blue beats Kasparov in second match (11 May 1997); long-term risks to the sanity of chess masters and the future of mankind?

• Microsoft Excel 97 re-exhibits ghost of Pentium FDIV bug (R 19 04,05)

• Microsoft Office 97 e-mail gives sight to blind copies (R 19 08)

• Microsoft Office 97 automagically transforms Michael Steffen Oliver Franz's initials 'msof' into 'Microsoft Office' (R 18 79)

• E-mail volume brings down MSN servers for C-E and T-Z names; Microsoft shut down entire service for several days to upgrade (R 19 09)

• Lots more on Y2K (R 18 74-80,82,83-84,87-88), including the unforesightful use of "12/99" as an out-of-band date flag (R 18 88); more on Y2K and other date/calendar/daylight arithmetic problems (R 19 02,03,06,08-12); costs to reprogram in UK (R 19 07); Y2K cost estimates worldwide now up to $600 billion (R 19 10)

• Windows 95 will crash in 2038 (R 18 84)

• More on European comma versus U.S. period in numbers (R 18 79)

• Studies of high-altitude cosmic-radiation effects on memory loss (R 18 79,81)

• A spelling-checkered existence: *WSJ* says Tony Blair "eLabourated" (R 19 12)

• More computer-is-never wrong tales (R 19 07,08); mad-cow disease database trusted more than reality (R 19 11)

SECURITY and PRIVACY

Newt Gingrich's teleconference compromised by cell phone (Bruce R Koball)

The New York Times reported on 10 Jan 1997 that Newt Gingrich was overheard in a telephone conference call to other House bigwigs on 21 Dec 1996 plotting strategy on how to deal with his ethics problems and possible attacks from opponents. This despite his promise, made the same day to the ethics subcommittee by his lawyer, that he would not use his office or his allies to orchestrate a counter-attack to the charges. The call had been recorded by a Florida couple from their scanner. [Not surprisingly, interesting controversies ensued about ethics, legalities of scanning, expectations of privacy, etc. See (R 18 75-76).]

Does CNID really give you anonymity?

From the time of an upgrade on 1 Jan 1997 until 26 Jan 1997, the mechanisms that are supposed to block Calling Number ID (misnamed Caller ID) failed in the 510 and 415 areas codes. As many as 516 businesses with PBXs were able to obtain calling numbers despite presumed blocking. [Source: *San Francisco Chronicle,* 14 Feb 1991. Watch out if you thought you were sending anonymous tele-valentines to companies with PBXs!] (Something on the order of 50% of the subscribers are rumored to have requested blocking.)

Taco Bell-issimo: salami-attack variant

Willis Robinson, 22, of Libertytown, Maryland, was sentenced to 10 years in prison (6 of which were suspended) for having reprogrammed his Taco Bell drive-up-window cash register – causing it to ring up each $2.99 item internally as a 1-cent item, so that he could pocket $2.98 each time. He amassed $3600 before he was caught. [AP item in the *San Francisco Chronicle,* 11 Jan 1997, A11, pointed out to me by Glenn Story.] This is a variant on the old salami attack, except that the long end of a few salamis disappeared instead of just a small slice of a lot of salamis.

Another privacy bug in Netscape (Kevin McCurley)

Version 2.0 of Netscape Navigator had a bug in it that allowed Websites to "steal" your e-mail address when you visited the page (see http://itu.rdg.ac.uk/misc/Mailing_Lists/cpd/00000002.htm). That bug was fixed in Version 2.02 by trying to require that the user approve any mail that is sent out from their machine. Unfortunately, a new bug has been discovered in Netscape 3.0, 3.01, and 4.0b1 that once again allows a Website to steal addresses from browsers without the consent of the user. A satirical demonstration of this was located at http://www.digicrime.com/noprivacy.html. [As usual, no guarantees are implied on the continued validity of old URLs. PGN]

ONE-LINERS:

• RSA crypto challenges: Ian Goldberg cracks 40-bit RC5 in 3.5 hours, using 250 machines to exhaust 100B would-be keys per hour (R 18 80); Germano Caronni cracks 48-bit RC5 in 312 hours, using 3,500 computers to search 1.5 trillion keys per hour (R 18 82).

• Emeryville Ontario cyberstalker (Sommy) (R 19 08) turns out to be family's son (R 19 10,11)

• NASA's Website hacked on 4 Mar 1997 (R 18 88)

• NCAA (Nat'l Collegiate Athletic Ass'n) Website hacked (R 18 90)

• David Salas, former subcontractor on a Calif. Dept of Info.Tech., was arrested on 3 felony charges for "allegedly trying to destroy" the Sacramento computer system (R 18 75,76)

• 3 Croatian teenagers cracked Pentagon Internet systems. Classified files allegedly stolen (?). *Zagreb Daily* suggests damaging programs could cost up to $.5M (?) (R 18 84)

• Dutch electronic-banking direct-debit scandal: Friesian church minister discovers surprise privileges (R 18 81)

• Stolen CalTrain ticket-by-mail computer contains sensitive customer data (R 19 02,05)

• Stolen Levi Strauss personnel computer contains 40,000 SSNs and other identifying info, also bank account into for retirees (R 19 12)

• Microsoft Network (MSN) users risk credit theft from fraudulent e-mail (R 19 08)

• Risks involved in Social Security Admin PEBES database (R 19 05,06,09,12); legislation to bar use of personal information (R 19 10); See PGN's U.S. House testimony on PEBES and identity theft (http://www.csl.sri.com/neumann/ssa.html), subsequent extended position paper for an SSA panel (http://www.csl.sri.com/neumann/ssaforum.html), and Chris Hibbert's SSN FAQ (http://cpsr.org/cpsr/privacy/ssn/ssn.faq.html). (R 19 12)

• Satellite monitoring of car movements proposed in Sweden (R 18 81)

• Swedish narcotics police demand telephone card database (R 19 07)

• Forged "PGP has been cracked" message (*not* from Fred Cohen); pursuing the given URL could lead to your ISP disabling you! (R 19 08,09)

• Moynihan Commission falls for Penpal virus hoax (R 19 04)

• Another risk of reusable passwords: sharing them to avoid Web fees (R 18 85)

• Dan Farmer's security survey [2 Jan 1997] catalogs attacks on government sites, banks, credit unions, etc. See http://www.infowar.com. (R 18 74)

• AOL4FREE.COM virus report started out as yet another hoax, but such a virus was created within 24 hours (R 19 11)

• More on risks in Netscape browsing histories (R 18 79)

• More on Java security (R 18 77,79,87); Another Java security flaw (R 19 11)

• Security problems in ActiveX, Internet Explorer, Authenticode (R 18 80-86,88-89); in particular, see detailed comments from Bob Atkinson (R 18 85) and subsequent responses (R 18 86-89); Paul Greene at Worcester Poly finds IE flaw (R 18 85); EliaShim notes two more IE flaws (R 18 88); Another ActiveX flaw (R 19 06,09)

• More on NT security (R 18 82,84,86-88); Another Windows NT security flaw (R 19 02)

• Chaos Computer Club demonstrates ActiveX/Quicken flaw on TV (R 18 80,81)

• More on Microsoft WORD macro security problems (R 18

70-72,75-77,79-89)
- Myths about digital signatures discussed by Ed Felten (R 18 83,84)
- Maryland attempting to outlaw 'annoying' and 'embarrassing' e-mail (R 18 81)
- Nevada contemplating outlawing unsolicited junk e-mail (R 18 87)
- Vineyard.NET spammed by VC Communications, sending 66,000 messages (R 18 79)
- More risks relating to spamming and spam blockers (R 19 02,05,10,13); legal implications (R 19 10)
- Phone calls to Moldova result from porn scam (R 18 80,83,84,87)

DIRECTOR, SOFTWARE DEVELOPMENT

Minneapolis-based, venture-backed, high technology company is currently accepting resumes for a **Director of Software Development**. This is a challenging position with opportunity for growth for an individual able to manage multiple engineering projects and project teams in new product development and/or customer specified product development.

The qualified candidate will have an undergraduate degree in engineering with recent development experience in Windows NT and 95 and ten or more years of UNIX, DOS, and Windows experience. An advanced degree in engineering science is preferred. The candidate should also be well versed in electronic data interchange and/or electronic commerce, design experience with data security products and software implementation utilizing public key cryptology. Additional experience is necessary in network security & security software, audit, and monitoring software architecture & design.

For confidential consideration send resumes to:
Kristine Olsen
P.O. Box 2106, Minneapolis, MN 55402
FAX: (612)305-5040
Email: Kolsen@kpmg.com

Report: 4TH ACM Conference On Computer and Communications Security

Donald J. Reifer, President
Reifer Consultants, Inc.

Introduction

The 4th ACM Conference on Computer and Communications Security [1] was held on 1-4 April 1997 in Zurich, Switzerland. About 100 participants from around the world gathered to discuss advances being made primarily in the area of defensive information warfare. This was primarily a research-oriented event which attracted principal investigators working in the security field from about 14 nations. I attended the conference for the following four reasons:

- I wanted to update my knowledge of the area.
- I wanted to ascertain what progress has been made in the field.
- I wanted to determine whether there were any breakthrough technologies on the horizon.
- I wanted to understand the threats being guarded against and the defensive strategies that leaders in the field were recommending.

As I will relate later, significant progress has been in many defensive information warfare areas. I particularly was impressed by the advances that have been made in the area of cryptography, digital signatures and communications protocols. I was disappointed by the perceived lack of progress over the years in the important area of trusted systems and information security infrastructure development.

This was the first conference that I have attended on the subject in about a decade. I selected the event because I thought that it would allow me to view both present work in the field and look into the future.

The Conference

The Conference began with a day of tutorials. I attended a morning session on the theory and applications of cryptography and an afternoon session on information warfare. Both were basic and summarized the field. The cryptography lecture was very enlightening. It discussed the Internet threats and how public and private cryptography key schemes help counter them. The information warfare lectures focused on defensive techniques; mainly because nobody seems to want to talk about offensive ones. It told us about how the good guys guard against and recover from breakins and active attacks. Speakers were knowledgeable and entertaining.

Two other tutorials were held. One focused on internet security architectures and the other on practical internet security for system and network administrators. I reviewed copies of both and found them interesting, but fundamental. The remaining three days was devoted to paper and panel sessions. Dr. Ross Anderson of Cambridge University's Computing Lab gave the keynote entitled: "Cryptography and security