ACM Fellows

ACM Fellow selections were announced recently. Dick Taylor, Lori Clarke, Lee Osterweil were some of the software engineering folks selected this year. To the best of our records, what follows is the list of ACM Fellows, who also are members of SIGSOFT.

- Paul W. Abrahams
- William R. Adrion
- R.L. Ashenhurst
- Victor R. Basili
- Lawrence Bernstein
- Barry W. Boehm
- Grady E. Booch
- James C. Browne
- Lori A. Clarke
- L. Peter Deutsch
- Larry E. Druffel
- Stuart I. Feldman
- Dennis J. Frailey
- Frank L. Friedman
- Richard P. Gabriel
- Susan L. Graham
- Cordell Green
- James J. Horning
- Richard A. Kemmerer
- Meir M. Lehman
- Nancy G. Leveson
- Joyce Currie Little
- Roger M. Needham
- Peter G. Neumann
- Davis S. Notkin
- Leon J. Osterweil
- Vaughan R. Pratt
- Barbara G. Ryder
- Fred B. Schneider
- Mary M. Shaw
- Eugene H. Spafford
- Guy L. Steele, Jr.
- Richard N. Taylor
- Albert J. Turner
- Chris S. Wallace
- Anthony I. Wasserman
- Jeannette M. Wing
- Stuart Zweben

The SENSational news is that a group of SEN associate editors (new volunteers) will be providing profiles/interviews of selected Fellows for future issues of SEN.

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
(1-650-859-2375; neumann@csl.sri.com)

From neumann@chiron.csl.sri.com Wed Nov 26 12:45:41 1997

Opinions expressed are individual rather than organizational, and all of the usual disclaimers apply. We address problems relating to software, as well as some cases involving hardware and other circumstances that affect computer systems. 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, or at http://catless.ncl.ac.uk/Risks/VL.IS.html [i.e., VoLume, ISsue] with a search engine courtesy of Lindsay Marshall. *SEN* archives are summarized at ftp://ftp.CSL.sri.com/illustrative.PS. [Although an earlier version of the summary appeared in the January 1996 *SEN,* it has grown too large to be included any longer.] 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 (1-650-859-2375; neumann@csl.sri.com; http://www.csl.sri.com/neumann/).

More on California's Deadbeat Dads' database

We noted in RISKS-19.12 and SEN 22 4 that there have been serious development difficulties in connection with SACSS, the California Statewide Automated Child Support System being developed by Lockheed-Martin IMS. The California Assembly continued to get inadequate answers on whether the system will ever work and how much more it would cost beyond the current 200% overrun to $300 million. The technical problems include human interface woes – the system has 357 screens and 57 ways of opening and closing them; data disappears, and sometimes migrates from one case to another; payments are miscalculated; and there were difficulties in communicating with other agencies. One additional risk was that if the system were not working adequately by the October 1997 deadline, California might lose 5% of its federal welfare funding. On the up side, Lockheed also developed a smaller system for Los Angeles (with 28% of the state's cases), and that system has been running successfully since early 1995. [Source: AP item in the *San Francisco Chronicle,* 21 Oct 1995, p. A21.] Finally, the California Health and Welfare Agency announced on 20 Nov 1997 that the Lockheed-Martin IMS contract has been cancelled altogether. [Source: *San Francisco Chronicle,* 21 Nov 1997, A30.]

Bug costs U.S. $3.8 million (David Kennedy)

The U.S. government has fired Hamilton Securities Advisory Services Inc. because of a computing error allegedly costing $3.8 million, and asked for retribution. In turn, HSAS firm defended its work for HUD, and claimed the department owed it $1.6 million for work successfully completed since 1993. [Source: HUD Firing, by Jennifer Rothacker, Associated Press Writer Courtesy of Associated Press via CompuServe's Executive News Service, AP US & World 21 Oct 1997, PGN Abstracting] The *Washington Times* reported on 20 Oct 1997 that the failure was in "erroneous instructions" to a computer model Hamilton used to evaluate the value of mortgage notes.

Medicare computer project terminated (Edupage)

The Clinton Administration has terminated the contract with GTE for a new computer system to handle Medicare because the current system (run by 72 private insurance companies around the country) proved to be so antiquated and complicated that they frustrated GTE's efforts. The Department of Health and Human Services has told GTE to "stop all work, make no further shipments, place no further orders, and terminate all subcontracts." Medicare officials say they will now work on individual pieces of the system rather than attempting to do the entire project at once. (*The New York Times,* 16 Sep 1997; 16 September 1997)

The risk of "zero defects" (Peter Kaiser)

I recently visited a Web page that contains this: "Cleanroom Software Engineering: The objective of the Cleanroom methodology is to achieve or approach zero software defects with certified reliability." The heading line was a link. I clicked on it, and got a page whose entire contents were: "Error opening file:" So I wrote to the Webmaster, who eventually responded that the problem had been corrected. I tried the link again. It hadn't. Perhaps by now it has been, but I'm in no hurry to go back there.

I'd be cautious in putting a page up about "zero software defects" – there may be some Gödelian rule operating in the universe of software under which any software complex enough to be useful must necessarily contain at least one defect. In *The Psychology of Computer Programming* (still a good read), Gerald Weinberg recounts a lovely story about debugging the null program. As you might guess, even the null program could contain bugs.

Network Solutions goof bumps Nasdaq off the Internet (Will Rodger)

The Nasdaq stock exchange was knocked off much of the Internet for several hours on 19 Aug 1997 as a result of administrative errors at the InterNIC, a centralized Internet address clearinghouse run by Network Solutions Inc. of Herndon, Va. Though the problem was initially invisible to Nasdaq, which maintains its own database of Internet addresses, the temporary suspension of access to the exchange's site blocked users of major computer networks – including those owned by IBM Corp., MCI Communications Corp., PSINet Inc. and UUnet Technologies Inc. As a result, Nasdaq was unreachable to most Internet users for at least several hours Tuesday morning. Problems with the Web site had no effect on the functioning of Nasdaq itself. The snafu was due to a clerical error at NSI, which evidently lost track of Nasdaq's $50 fee, submitted in October 1996. [PGN Abstracting, from article by Will Rodger, in Inter@ctive Week Online, 21 Aug 1997]

Will remarked that things like this seem to be occurring more often. The weekend before, more than 5,000 Web sites were blocked for over 24 hours, when Web Communication Inc and other domains were bumped from the Internet after a screwup in routine InterNIC maintenance.

Rough days on the stock markets (PGN)

With the huge fluctuations in stock prices on 27-28 Oct 1997, the NYSE and Nasdaq each handled over a billion shares for the first time ever on 28 October 1997, with the NYSE at 175% of the previous blockbuster day. The bad news is that those folks who relied on the Internet to do their panic trading were in for a rough time. There were huge numbers of e-trades already queued up before opening, causing an early traffic jam. Joseph Konen of AmeriTrade Holding blamed some of the delays on limitations of its firewall technology. Many would-be Internet buyers and sellers simply could not get access, in part because their Internet service providers were saturated. Many customers were blocked out because others were tying up lines just to monitor the market. (Illustrating the extent to which Internet trading has become a part of the markets, Schwab normally does 35 percent of its trading on-line; yesterday's trading of more than 300,000 online transactions more than doubled their Monday load and tripled their typical day.) Conventional trades were also affected. [Steve Bellovin, Frank Carey, and Nick Bender gave lots of details, including Nick noting the effects on Nasdaq of a sequence-number overflow from 999,999 to 000,000 (R 19 44).]

Explosion causes Internet blackout in New England

More than 200 New England businesses experienced a four-hour Internet blackout on 7 Aug 1997 after an explosion knocked out electrical power in the Boston area. One person was killed in the blast, which overloaded a panel switch at MIT, causing a fire and cutting off Internet access to BBN Planet customers. Access resumed around 10:00. The speed with which the incident happened made it impossible to reroute traffic, said a BBN spokesman. (*TechWire,* 8 Aug 1997; Edupage, 10 Aug 1997)

MFS Communications switch fails, with widespread effects (Steven Bellovin)

Around 7 p.m. on the evening of 8 Sep 1997, the main MFS Communications switch (MFS Switch One) failed, downing UK telecommunications links provided by MFS, Worldcom, and First Telecom. The outage also affected most of CompuServe's UK customers, whose access is typically via an MFS phone number. [PGN Stark Abstracting. Evening usage is not necessarily off-peak, because it is an excellent time to ac-

cess computers in the U.S. No one has yet reported how long it took to restore service. PGN]

Satellite transmission snafu leads to diplomatic incident (Nick Brown)

On 19 Jul 1997, a "technical error" caused the contents of a channel on a satellite (operated by France Telecom) to be transmitted on another channel, for about twenty minutes. Normally this would have been merely annoying for the viewers. However, these viewers were in (among other places) Saudi Arabia, the channel they expected to be watching was the French government-run, general interest and news station, Canal France International (CFI), and the program which replaced it was a hard-core pornographic movie that should have been shown on the subscription-only, encrypted French domestic station, Canal Plus. As a result, Arabsat cancelled its contract with France Telecom, claiming that France Telecom had not "honoured its commitment to respect Arabic and Islamic values." The French Foreign Ministry and the French Ambassador in Riyadh are trying to calm what has become a diplomatic incident.

Indian satellite failure (Scott Lucero)

According to the 6 Oct 1997 *Daily Brief,* officials in India say the country's most advanced communications satellite was abandoned on 5 Oct 1997 due to a power failure aboard the craft. The loss of the satellite reportedly affected communications to remote parts of the nation and the operation of satellite-dependent functioning of India's stock exchange. This appears to be an example of the familiar RISK of having a single point of failure, or, more colloquially, putting all your eggs in one basket.

No network, no demo (Martin Minow)

Larry Ellison, CEO of Oracle Inc, and a strong proponent of network computers, was demo-ing his network computer at the Oracle OpenWorld conference. Unfortunately, the network crashed and the application hung "and Ellison was left hanging on stage."

Korean Airlines KAL 901 accident in Guam

The Guam KAL 801 crash killed 225 of 254 on board. A bug was uncovered in upgraded software that had existed worldwide (R 19 29), relating to incorrect barometric altimetry in the Ground Proximity Warning System (GPWS). See a detailed analysis by Peter B. Ladkin and other discussion (R 19 37-38).

Union Pacific rolling (?) stock (Daniel P. B. Smith)

Following Union Pacific's assimilation of Southern Pacific, to form the nation's largest railroad, UP has been unable to accurately track its freight cars, resulting in gridlocks and lost trains – most visibly in the southern corridor from LA to Texas, the Gulf Coast region, and the central corridor from Oakland to Chicago. There are major bottlenecks in LA, North Platte, Chicago, and Houston. Integrating the computer systems was reportedly "more difficult than anticipated."

There are many horror stories, including a load of liquid gas that had "virtually evaporated into thin air by the time it arrived;" it took 51 days to ship a load of plastic resin from Dallas to Forth Worth; a shipment from Memphis to California by way of Little Rock, then Memphis, then Little Rock, then Memphis, then Little Rock, then El Paso... Mr. Lundgren of Englin Cotton Oil Mill reported watching one of his own freight cars on UP tracks barreling past his office. "A few days later, he saw it pass again in the opposite direction." [Culled by PGN from Daniel's submitted item by Anna Wilde Mathes and Daniel Machalaba, *Wall Street Journal,* Monday, 13 Oct 1997, p. B1, and another detailed item by Carl Nolte and Kenneth Howe, *San Francisco Chronicle,* 11 Oct 1997, D1. Massive grain backlogs and storage problems were also noted (R 19 43).]

Mad-bus disease (Geert Jan van Oldenborgh) Nine people were injured, one seriously, when a Dutch long-distance bus suddenly accelerated from the bus terminal behind Eindhoven Central Station, and ran into the station restaurant. The builder acknowledged that these sudden accelerations were a known problem, he suspected that it had something to do with interference on the electronic accelerator pedal by the communications equipment, the 2-way radio, the mobile telephone and/or the little box which operates traffic lights. No technical shortcomings had been found in previous inspections, but the busses still career out of control every now and then... The worst-affected 22 out of 178 have now been taken out of service. [source: NRC Handelsblad, 25 and 26 sep 1997].

Two out-of-band comments: in case you wondered, a long-distance bus is defined locally as one that goes more than 50km. The linear dimensions of our country are about 200km... Secondly, with regards to the computer-operated storm-surge barrier I reported on earlier, a week later it transpired that the software was not yet ready in fact, and would become operational this autumn. Until then a human would decide when to close off Rotterdam harbour. Fairly typical I assume... GJ

Computer malfunction floods Boulder garages and basements (S.J. Hutto)

"Officials blamed a malfunctioning computer for five water main breaks late Saturday that cut service to about 40 homes, flooded basements and garages and turned city streets into rushing streams." A computer controlling water pressure gave inaccurate readings, prompting a city worker to open up the mains. [Source: *Rocky Mountain News,* 25 Aug 1997]

Nielsen snafu hurts cable network's ratings (George Mannes)

A "software snafu" at Nielsen Media Research, the company responsible for TV and cable ratings, undercounted the viewers of the USA Network on a daily basis from April 1 through July 1, according to a report by Richard Huff in the 4 Sep 1997 *NY Daily News.* The overlooked viewers, about 15,400 homes each day, were in homes with DirecTV satellite systems. The

article estimates that the undercount cost USA Network $2 million. "It was a very unique and unusual circumstance, technical in nature," said a USA Network executive quoted in the story. Correcting USA's ratings, according to the story, is impossible, because "all DirecTV viewing information about USA was lost in the computer foulup."

Risk of not updating Web pages (John Oliver)

I have been trying to get information about courses at one of the major Australian universities. The Web site lists X as the contact person for the Faculty of Arts. All mail to X bounces with a message that the mail spool is full. After weeks of trying, I finally found someone who would read my complaint about it and check. It turns out that X is on maternity leave and no one changed the Web page.

Risks of civic virtue (Peter Wayner)

I paid too much in taxes and got labeled a deadbeat taxpayer. Here are the four components for disaster: 1) my mortgage holder pays my property taxes, 2) I'm enrolled in a special program that lowers the amount kept in escrow because I pay these taxes semi-annually instead of annually, 3) most people pay annually, 4) computers. The mortgage company, for some bizarre reason, paid too much in taxes. It turns out they paid the 3% fee for using the semi-annual scheme with the first half instead of the second half. The city's computers saw that the amount was more than was owed semi-annually and assumed I was voluntarily trying to pay annually. It kindly switched me over to the annual plan. But since the amount was also less than the annual amount, it assumed I was a tax cheat. If I didn't catch this, the house would have been auctioned off.

Stansfield Turner's new book includes near-war risk

Admiral Stansfield Turner's book, *Caging the Nuclear Genie,* describes an incident that occurred on 3 June 1980 when he was President Carter's CIA director. Colonel William Odom alerted Zbigniew Brzezinski at 2:26 a.m. that the warning system was predicting a 220-missile nuclear attack on the U.S. It was revised shortly thereafter to be an all-out attack of 2200 missiles. Just before Brzezinski was about to wake up the President, it was learned that the "attack" was an illusion – which Turner says was caused by "a computer error in the system." His book makes various suggestions that would greatly reduce the threats of accidental nuclear war. "We have had thousands of false alarms of impending missile attacks on the United States, and a few could have spun out of control." [Source: Keay Davidson, *San Francisco Examiner,* in the *San Francisco Sunday Examiner and Chronicle,* 19 Oct 1997, p. A-17.]

ONE-LINERS:

•Mir Space Station computer problems add to difficulties; main computer failed during docking attempt, 19 Aug 1997 (R 19 31,32), with detailed analysis by Dennis Newkirk (R 19 33)

•More on risks of RF interference in aircraft: cell-phone linked to London to Istanbul crash-landing? (R 19 34,36,37)

•New York air traffic slowed for 10 hrs by construction contamination (R 19 41)

•GM sudden acceleration (31 deaths, 1121 injuries between 1973 and 1986) linked to EMI in court; Audi cases still suspected; cars less protected than aircraft (R 19 38); note from Adam Cobb in Australia (R 19 42)

•Remote-control car starter also controls car doors, turns on heater, defroster, or air-conditioner, up to 400 feet away (R 19 37)

•Swedish policeman's handheld digital radio triggered his car airbag, which hit him with the radio unit (R 19 43)

•Channel Tunnel closed in both directions on 20 Aug 1997, cause not reported (R 19 32)

•Effects on automated traffic controls of plane crashing into 500Kv power line near Cajon Pass; more than 1000 traffic lights out (R 19 29,30); earlier effects of power failure in Perth (R 19 30); risks of major outages (R 19 32,33)

•Cold weather impairs fiber-optic performance (R 19 41)

•Blizzard cuts life-support, traps Lakin, Kansas, girl, who dies (19 44)

•More than 150 cases of falsified reports on welds in nuclear-power plants. (R 19 39)

•After-effects of the Tamagotchi e-pets; more than just a game? (R 19 36,37)

•Risks related to Ctl-Alt-Del (R 19 28,29,31,32)

•Bug in DoD Common Operating Environment screen-lock consumes resources (R 19 42); NT screen savers also risky (R 19 43)

•New Pentium flaw enables user-mode program to lock up the system (R 19 45); preventive fixes in operating systems, software (R 19 46,47)

•Centaur IDT-C6 Pentium-compatible: "exacting proof of correctness" results from tests on PC OSs because of their complexity! (R 19 25)

•Faster Mac reveals lurking flaw (R 19 38,40)

•Lynx 2.7.1 browser on mistyped URLs coerces http.org domain (R 19 42)

•Discussion of local classes in Java, flaw and fix (R 19 41,42)

•Risks of banks' not retaining data between Quicken runs (R 19 39)

•"Computer error" affects hundreds of UK A-level exam results (R 19 40)

•SP? Laptops on the Senate floor: fears of surfing, lobbyists, etc. (R 19 29,32,33)

•ISO 8859-1 7-bit vs. 8-bit incompatibilities (R 19 40)

•Y2K: Tcl 8.0 bytecode compiler Y2K risks; 00-38 now 2000-2038 (R 19 35-37); Y2K and C (R 19 37-38,40); non-Y2K problems with Java Date classes (R 19 38)

•DoD Global Command and Control System (GCCS) fails Y2K test (R 19 38)

•Y2K lawsuit: Produce Palace International sues Tec-America (R 19 29)

•Daylight-savings: falling back 1997 – VCRs, Interac ATMs, Win95 (R 19 43,44)

•Hospital computer crashes every midnight at midnight until 00:15 (R 19 25)

•AOL off line for two hours 29 Oct 1997 (R 19 44); AOL e-mail outage due to software, 3 Nov 1997 (R 19 45)

•Judge Zobel's awaited e-mail in "au pair" case delayed over an hour by Boston Edison Electric workers in a manhole disconnecting his ISP (R 19 45)
•More spelling curiosities: *semper fidelis* corrected to *semipro fiddles* (R 19 34-36); html mangling of & character (R 19 35)
•US West discovered its 911 lines were too silent, added noise (R 19 41); similar problem with Lexus engines (R 19 42)
•More machines phone home: summary notes cold drink dispensers, lonely oil tank, faulty public lavatory, medical insulin fridge alarmed because of low temperature (R 19 31,33); multiple autodial illegal (R 19 36)
•Risks of errors in Calif Megan's Law CD of sex offenders (R 19 25)
•GSM phones recalled for software upgrade (R 19 27,30)
•Northern Telecom DMS-100 billing errors result from upgrade (R 19 38)
•More nonatomic ATM transactions: account debited, no cash (R 19 40)
•Upload of flawed AT&T SS7 translation database took out 800 service (R 19 39)
•Ordering airline tickets on-line: Nonatomic transaction gave tickets but no reservation (R 19 27); name confusions on e-tickets, with similar names (R 19 28) and identical names (R 19 29)
•IRS incorrectly warns 90,000 taxpayers of Nannygate delinquency (R 19 28)
•When it was automated, Paris police computer mismatched split-out Corsican city code with postal code, and was unable to collect motorists' fines (R 19 41,42)
•QuickTax 97 miscalculates self-assessment taxes (R 19 30)
•Risks of Florida's automating traffic citations (R 19 34)
•Reactions to Mary Schmich's parody of Kurt Vonnegut on the Internet (R 19 29)
•Added note on risks of systems maintenance taking place in a different time zone (re: .COM, .NET DNS tables) (R 19 35)
•Hong Kong Flying Service computer systems corroded by hydrogen sulphide (R 19 41)
•Rat-inducted short-circuit at Barranquilla airport closes airport (R 19 38)

SECURITY and PRIVACY

The Eagle (the President) and the Eagle Beagle (David Wagner)

An unidentified hacker announced on 19 Sep 1997 the interception of President Clinton's pager messages (along with pager messages destined for staff, Secret Service agents, and other members of his entourage) during his April 1997 trip to Philadelphia. The lengthy transcript of pager messagers was published on the Internet to demonstrate that the pager infrastructure is highly unsecure.

(Apparently the President's entourage relies a lot on pagers for communications. There are messages from Hillary and Chelsea; a Secret Service scare; late-breaking basketball scores for the President; staffers exchanging romantic notes; and other amusements.)

This comes at quite an embarrassing time for the administration, given their policy on encryption. Strong encryption is the one technology that could have protected the private pager messages, but the administration has been fighting against strong encryption. Top FBI officials have been giving many classified briefings to House members, asking them to ban all strong encryption in the US.

An anonymous White House staffer was quoted as saying that it would be "an expensive and complicated proposition" to put encryption into pagers and cellphones. This quote is interesting, because it's the White House's crypto policies that have made it so complicated and expensive to add strong encryption – the cellphone and pager industries have wanted to add strong encryption for privacy and security, but the administration has forcefully dissuaded them from doing so. [Adapted from a cypherpunks item, with David's permission. See RISKS-19.39 and 40 for more, and check out my Web pages for my recent Senate and House testimonies on risks in the computer-communication infrastructures. PGN]

Prosecution for pager interceptions (Steven Bellovin)

A New Jersey company has been charged with illegally intercepting and selling messages sent via a paging service. The messages – the content of which was sold to news organizations – were intended for delivery to the offices of various senior New York City officials, including the mayor's office and various top police and fire department officers. (See R 19 35,36 for the rest of the story.)

San Francisco blackout blamed on sabotage

126,000 customers in northern San Francisco experienced a power outage for up to 3.5 hours beginning at 6:15 a.m. on 23 October 1997, when five transformers stopped working at the power substation at Eighth and Mission. The FBI counterterrorism unit is investigating what it considers the likelihood of sabotage (for reasons not revealed, although 39 of the 42 switches were open).

Federal Web sites lack privacy safeguards (Edupage)

OMB Watch, a nonprofit group that monitors government activities, faults the federal government for its lackadaisical approach to protecting the privacy of government agency Web site visitors. "There is no government-wide policy regarding privacy concerns on federal Web sites... Agencies collect personal information about visitors to their Web sites, but fail to tell them why that information is being collected and what it is being used for," says an OMB Watch information specialist. Nearly half of 70 federal agencies collect information about their online visitors, but only 11 inform them how that information will be used. Three agencies, including the National Science Foundation, were collecting cookies – a set of data that enables the Web server to track a user's patterns and preferences – but all three have stopped following the release of OMB Watch's draft report. (TechWire 27 Aug 1997; Edupage, 28 August 1997)

RC5-56 cracked (David McNett)

"It is a great privilege and we are excited to announce that at 13:25 GMT on 19-Oct-1997, we found the correct solution for RSA Labs' RC5-32/12/7 56-bit secret-key challenge. Confirmed by RSA Labs, the key 0x532B744CC20999 presented us with the plaintext message for which we have been searching these past 250 days.

The unknown message is: It's time to move to a longer key length

In undeniably the largest distributed-computing effort ever, the Bovine RC5 Cooperative (http://www.distributed.net/), under the leadership of distributed.net, managed to evaluate 47% of the keyspace, or 34 quadrillion keys, before finding the winning key. At the close of this contest our 4000 active teams were processing over 7 billion keys each second at an aggregate computing power equivalent to more than 26 thousand Pentium 200s or over 11 thousand PowerPC 604e/200s. Over the course of the project, we received block submissions from over 500,000 unique IP addresses. [...] Adam L. Beberg - Client design and overall visionary; Jeff Lawson - keymaster/server network design and morale booster; David McNett - stats development and general busybody" [excerpted for *SEN*]

Ghost account nets $169K embezzlement

While working as a civilian military pay supervisor in the Army finance and accounting office at Fort Myer from 1994 to 1997, Teasa Hutchins Jr. caused regular military paychecks to be deposited to a bank account in the name of a bogus officer, and accumulated $169,000 for himself. He has pleaded guilty and faces up to 10 years in prison and a $250,000 fine. [Source: An item in *The Washington Post,* summer 1997.]

24 more California DMV clerks fired in fraudulent license scheme

The California DMV has fired 24 more clerks who accepted bribes to issue driver's licenses fraudulently. This brings the total to 79 in the current statewide probe, Operation Clean Sweep. The going rate was $200 to $1000 a pop for not checking the applicant's identity, typically paid by illegal aliens, felons needing new identities, and drivers with revoked licenses. [Source: *San Francisco Chronicle,* 1 Aug 1997, A25]

Masquerader's name collision lands robbery victim in jail

Antonio Picazo Mendoza Jr., was beaten and robbed on his way to a store near his home in Stockton, California. He managed to get home, where his family reported the robbery to police and took him to the hospital. Police discovered that his first and last name, date of birth, and Social Security Number matched those of Antonio Blanco Mendoza, a wanted parolee. Despite his protests that he was not that individual, he was detained in jail – for three days by the San Joaquin County Sheriff's Office, and for another two weeks at Deuel Vocational Institution. It appears that Blanco was using Picazo's identity. [We have had numerous cases in the past of *intentional* identity theft and *accidental* assignment of the same SSN to different individuals. It is not yet clear which is true in this case.]

Another phony-fax get-out-of-jail scheme

Richard Foster, jailed for driving with a suspended licence, was set free from South Carolina's Richland County jail – based on a fax with an "official-looking sheriff's letterhead". The fax stated that Georgia's Augusta-Richmond County Sheriff's Office had no interest in Foster. (Actually, at that time he was wanted on assault and weapons charges.) The fax had been sent from a public fax machine at a Kroger grocery store in Augusta GA, and had the Kroger name and phone number on the fax. As a result of this spoof, the jail supervisor has been demoted from captain to sergeant. [Source: *San Francisco Chronicle,* 23 Jul 1997, A2] [Similar cases are recorded in Florida (RISKS-18.94) and Tucson AZ (RISKS-12.70).]

Another computer-miscontrolled jail (Scot Wilcoxon)

The *Minneapolis Star Tribune* reported on 27 October 1997 on the likely reasons behind the escape of a prisoner from the Carver County jail on 2 Oct. When a guard pressed buttons to let another guard through a door, he also bumped the button for an external emergency exit. The external door became unlocked, and air pressure popped it open. Several prisoners chose to stay in the room, and one escaped for a day. Opening that external door was supposed to require pressing a "door open" button, two "interlock open" buttons and then the button for the specific door. Somehow that door did unlock when its door button was bumped while an internal door that requires only pressing two buttons was being opened. Authorities were later able to open the door that way several more times.

An internal investigation has not been completed, but three explanations were offered:
1. Reprogramming of operational software controlling internal doors may have inadvertently changed functions affecting the door.
2. Lightning struck the jail this past summer, which resulted in a power failure and a computer-system crash. Some of the software may have been damaged when the system was rebooted.
3. All the functions were tested when the system was installed over two years ago, but tests were not made to see if the door could be opened by hitting other buttons.
Doors are also serviced after they've been opened 5,000 times, which makes it easier to detect if one isn't working. But this external emergency door has only been opened five times, with a key, for maintenance.

Risks of offshore Internet gambling

As of August 1997, there were reportedly at least three-dozen Internet gambling houses, the latest of which – Bet the Net – began operating as an Internet casino from Dominica in the Caribbean. The expected revenues from all such Internet operations is estimated at $8 billion by the year 2000, where the current total take for U.S. casinos is currently $23 billion.

[Source: Bloomberg News, *San Francisco Chronicle*, 1 Aug 1997, B2.]

The risks include bogus virtual casinos whose payoffs turn out to be more virtual than real, semi-legitimate casinos working credit-card scams on the side, glorious opportunities for money laundering, serious gambling debts accumulated in your name by a masquerader, spawning of serious undetected addictive behavior that might otherwise be observed (on the Internet no one knows you are a gambler, except for the casino), your 9-year-old gambling with your credit card – especially if your browser automagically inserts your credit information – and so on into the night. As a second-order effect, massive illegal activities could also lead to attempted restrictions on the good system security and cryptography necessary to conduct legitimate Internet commerce. In any event, whether or not you bet on the Net, don't bet on the Net being adequately secure! You are already gambling with the weaknesses in our computer-communication infrastructures, but NetBet could raise the ante considerably. Caveat aleator.

ONE-LINERS:

•Social Security Administration restores PEBES service, with a few opt-in and other safeguards (R 19 37)
•AOL hit by e-mail scam and Trojan horse URLs (R 19 34)
•AOL announces its intent to share data with telemarketers (R 19 26) and ads on private e-mail (R 19 40)
•Trojan horse: 5-yr-old installs AOL CD-ROM from Chex Quest box (R 19 26)
•Win 95 Microsoft TCP/IP flaw freezes system (R 19 26)
•Beware of offer of remote Active-X-enabled antivirus scanner (R 19 30)
•Netscape Communicator 4.01 for Windows 95/NT risks include forgeable digital signatures (R 19 30)
•Netscape Communicator 4.02 and 4.01a allow disclosure of passwords (R 19 34)
•Risks in Secure Electronic Transaction (SET) protocol (R 19 31-36,48)
•Thieves profit from $240,000 in debit-card transaction adjustments (R 19 42)
•Implications of outlawing concealed messages: ban the Bible, smiley faces, foreign languages (Navaho used in WWII), online card catalogs, random numbers, what else??? (R 19 37-41); use of steganography, e.g., in graphical images (R 19 40,41); Feynman's censors in WWII objected to math! (R 19 39)
•More on risks of key recovery: see also PGN testimony of Senate Judiciary Committee and responses to questions (http://www.csl.sri.com/neumann/)
•More on cryptographic hashing and MD5, Paul Kocher (R 19 26)
•More on risks of voice-controlled human interfaces (R 19 25)
•Overload caused Experian credit reports to go to wrong people (R 19 31)
•Microsoft Trojan horse in Office97 installation (R 19 29)
•Microsoft Internet Explorer flaw due to violation of Java VM (R 19 29)
•Deutsche Telekom T-Net-Box answering-machine security problems (R 19 29)
•Security flaw in Rogers Cablesystems Wave gives access to other users' data (R 19 43)
•Mobile-phone electromagnetic radiation causes short-term memory loss; related to talkers' road accidents? (R 19 39)
•PBS and TV "Barney & Friends" signal to activate interactive Barney doll via Microsoft ActiMates set-top box (R 19 39)
•GPS privacy issues (R 19 29); GPS lost time synch when first activated when cleaning crew unplugged the master time source! (R 19 30)
•Hong Kong accidentally releases journalists' personal info (R 19 28)
•4-star General Griffith's SSN posted on Internet site (R 19 28)
•Carlos Salgado Jr. pleads guilty, max up to 30 years, $1M fines (R 19 34)
•Washington State posts criminal history records on the Net; legal issues (R 19 28)
•Bank robbery "wanted" poster of wrong person due to unchecked match (R 19 29)
•Knowledge of SSN sufficient to convince SSA falsely of Kirsten Phillips' death (R 19 39)
•Computer system implicated in need for death-penalty review (R 19 29)
•Spams and associated risks (R 19 25,27,31-34); laws (R 19 35-36); $125 million lawsuit to stop striptease advertising via Strong Capital Management (R 19 27); Hewlett-Packard scanner spam (R 19 38); Pacific Bell Internet spammed with forged QueerNet address, causing Pac*Bell to misdirect its retaliation (R 19 44); Samsung spam and reverse-spam (R 19 32,33)
•Discussion of whether U.S. Code Title 47, Section 227 applies to spam (R 19 33-36,42,44)
•Discussion of leaked report on Mondex security flaws (R 19 38)
•- Gerber net hoax (R 19 43)
• Wendell Dingus sentenced to 6 mos home monitoring for cracking USAF and NASA computers from Vanderbilt U. (R 19 35,36)
•S+$ "Crack a Mac" contest server cracked; winners get 100,000 Swedish kronor each (R 19 31)
• Czech intelligence computer stolen, with sensitive data (R 19 31)
• Alaska exposes its rascals on Web site (R 19 30)
• Password unsecurity in NT cc:Mail release 8 (R 19 37)
Risks of Web sites from computer fraud (R 19 44)
• Victim ordered to surrender computer and passwords (R 19 43)