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, and (R i j) denotes RISKS vol i number j. Volume 22 is 1997. The RISKS archives are available on ftp.sri.com, cd risks. 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.

Bright Field crash in New Orleans computer related (PGN)

According to John Hammerschmidt of the National Transportation Safety Board, preliminary investigations into the freighter *Bright Field* crashing into the Riverwalk in New Orleans suggest that an oil-pump failure caused the ship's computer to automatically reduce speed. A standby pump kicked in, but under reduced power the ship's maneuverability was decreased. The impact cut a 200-foot swath into shops and a hotel condominium complex, and the pedestrian walkway. A language barrier between the Chinese-speaking captain (and crew) and the English-speaking pilot reportedly may also have contributed. The Liberian-registered 69,000-ton ship was not equipped with a U.S.-recommended voice recorder, and a second voice recorder was not functioning. Coast Guard Captain Gordon Marsh confirmed that large ships lose steering power as often as once a week. [Source: various news items, including *San Francisco Chronicle,* 17 Dec 1996]

(David Lesher:) The pilot appears to have performed a miraculous job of parallel-parking the 761-foot vessel in the 900-foot space between two heavily populated entertainment boats. The risk? While the automatic reactions clearly saved an engine that likely costs millions to rebuild, could the sacrifice of the engine have prevented the collision? Or would the engine have exploded, throwing *large* pieces around and killing people that way?

(Michael Quinlan:) "The captain also acknowledged forgetting he had a computer override button on his console that could have allowed him to bypass the computer and increase the ship's speed and maneuverability."

BART software crash and system delays (PGN)

Bay Area Rapid Transit (BART) had another bad day. At 7am, a ghost train (one that isn't really there but that the computer believes *is* there) appeared at the San Francisco 24th Street station, requiring manual operation through that station. Independently, three trains had to be taken out of service because of mechanical problems. All of this caused a 15-minute delay systemwide. Later, a computer crash caused delays up to 30 minutes systemwide, from 5:50pm to 9:45pm on 19 Dec 1996. (RISKS archives include various ghosts, including recurring problems in the San Francisco Muni Metro and in the Chunnel.)

Incidentally, Andrew Waugh noted (R 18 74) that a 'ghost train' is most likely due to a track circuit failure, which suggests a fail-safe design that detects a train when it fails rather than failing to detect a real train – ergo, a RISKS success story!

BART also had a serious power cable outage in the transbay tunnel on 12 Dec 1996. That cable problem was traced to sloppy maintenance after the cable was damaged way back when it was installed in the early 1970s. BART management observes that an overall cable overhaul had been considered prior to the 12 Dec outage as an urgent step in upgrading the aging infrastructure.

Nick Brown (R 18 70) wrote a nice piece on the effects of aging on computer-related systems, inspired by various relevant RISKS items. Check it out.

S-Bahn stopped by new switching software (Debora Weber-Wulff)

The *Berliner Tagespiegel* reported this week on the new light-rail switching software that was installed the same weekend that the light rail (S-Bahn) was moved back from the regular train track to its own tracks, which had been under repair for some time. The tracks were cut off all day Saturday and Sunday with buses attempting to move passengers. The software is installed at a central switching board, so that the transportation company can save the money they would otherwise pay real people to manually move the switches. The software kicked in, and Monday all went well until rush hour hit – yep, you guessed it, a stack overflow, just like in Hamburg. And it is the same large German company that was responsible for the Hamburg fiasco that wrote this software – it may even be the exact same software. Will they ever learn to *do* quality assurance at this company and not just talk about it? It took hours to get the system back up. The newspaper quotes (ironically?) a spokesman as saying that the software control was very modern since there is only one point at which it can go wrong. Of course, if that single point goes wrong... I spoke with a nameless higher-up at the transportation company, who just said "Software always has errors. We're just happy that no one gets killed when the software fails."

Amtrak ticket system breaks down (PGN)

On Friday, 29 Nov 1996, Amtrak's nationwide reservation and ticketing system was rendered almost useless by a breakdown in the network, during what is usually the heaviest travel weekend of the year. The outage caused enormous confusion

and delays, because agents typically had no printed schedules and fare tables, and had to issue tickets by hand! [Source: An item from *The New York Times* in the *San Francisco Chronicle,* 30 Nov 1996, A6.] (See R 18 64, refinement by Bob Perillo R 18 67.)

Cutting off husband's cybersex leads to assault (Mich Kabay)

When Marion Walton, an Arkansas man, was discovered having a cybersex affair with a Canadian woman, his wife Pat apparently erased his e-mail program. In retaliation, he apparently beat her, twice. "Police are suggesting she file charges." [Another risk of program erasure! Source: Reuters World Report, datelined Little Rock, 31 Oct 1996, via CompuServe's Executive News Service, PGN Abstracting.]

Limits of automated newsgathering (Terry A. Ward)

"Rugby Union-Canadian Hooker out in the Cold. Canadian international hooker Karl Svoboda has been ousted from the Oxford team to face Cambridge University in the showpiece Varsity match at Twickenham ..." [Source: A Reuters item from the NewsPage Direct automated news service for Human Sexuality, evidently confusing a rugby position with a sex-worker's position. This is a really scrum-ptious item! PGN]

California tax-form attacks: a new tax on businesses (PGN)

A California Franchise Tax Board computer system apparently went berserk, resulting in thousands of extra copies of 1996 tax forms being sent to California businesses – including a San Diego dentist who reportedly received about 16,000 copies of the 1996 forms. [Source: An AP item in the *San Francisco Chronicle,* 14 Dec 1996, A16.]

Shetland Islands newspaper hyperlink controversy (Lance Hoffman)

The Shetland Islands have a 124-year-old print weekly (*Shetland Times*) and a 1-year-old online daily (*Shetland News*). The *News* includes titles of *Times* articles as hypertext links to the *Times.* Robert Wishart, the *Times* managing director (who once fired his former editor, Jonathan Wills, who is now the *News* publisher), has demanded that the links be removed; Wills has refused, although he did add asterisked footnotes. Wishart then invoked Scotland's Court of Session, which issued an interim interdict against the hyperlinks. A full hearing is pending. If the interim judgement is upheld, this is seemingly a landmark case in Scotland and potentially the UK, including issues such as the differences between a web site and a cable TV service, and whether newspaper headlines constitute copyrightable literary works. [Source: Scottish Case Tests 'Right to Link', By Pamela Mendels, *The New York Times* CyberTimes, 30 Nov 1996. PGN Abstracting]

San Jose garbage billing system snafu (PGN)

San Jose, California, issued no garbage bills (186,000 homes and 3765 apartments) after the beginning of October 1996 – because of "faulty procedures in saving backup records." The city is spending $360,000 to rectify the situation, which was estimated to take until mid-December. [Source: *San Jose Mercury News,* 13 Nov 1996, courtesy of Babak Taheri.] Garbage collections continue, while revenue collections do not.

Washington State Unemployment Checks "Delayed" (Richard Berry)

A state computer might be the Grinch that is stealing Christmas for some unemployed people. The computers that began to process claims for unemployment insurance at the end of November have "mislaid" checks (up to $365) for up to two-thousand jobless people. Employment Security commissioner Gary Moore notes that tens of thousands of checks were properly sent out. He says the system works well, but has some bugs that need to be worked out. But Moore also acknowledged that people who haven't gotten their checks need the money, and waiting for checks from the state is unacceptable. [From the KOMO radio/television station news website, 12 Dec 1996]

Computer malfunction causes panic selling at Hong Kong stock exchange (Joel Chan)

A computer glitch in the Hong Kong Stock Exchange caused panic selling on 12 Dec 1996 when its Teletext information system incorrectly reported a drop of 515 points (or about 4%) of the Hang Seng Index during the opening minutes of trading. The error was blamed on a malfunction in the Automatic Order Matching and Execution System (AMS), which calculates up-to-the-minute stock prices during trading hours. The Stock Exchange had apparently alerted dealers that there was a problem with the computer before trading began and advised them to use prices shown in free-text areas for calculating opening quotations. However, the Teletext system made no indication of the computer glitch and instead displayed inaccurate stock prices until 20 minutes after trading began. The stock exchange is reviewing the incident.

Mobile phone mayhem: running interference! (Trevor Warwick)

Another twist on the well known "Cleaner buffs computer room floor and takes down entire site" stories: We recently had some engineers from AT&T in our computer room for three days, working on a PABX which also lives in there. During this period, two of our main Netware servers were extremely unreliable, crashing several times a day. The AT&T engineers were working near these servers, and we initially thought that they might have been causing the crashes by disturbing some cables. After a few of these unexplained crashes, one of our MIS group noticed that every time he went into the server room to reboot the dead servers, one of the AT&T engineers was using his mobile phone. So, they were asked to turn their phones off while working in the server room, and the problem has not recurred. To test the theory a bit further, the MIS group then took an otherwise unused server, and experimented with using a mobile phone near it. With the working phone being used less than a foot away from the machine, they provoked a crash – which corrupted the system disk (and its mirror volume) beyond repair.

Bell Atlantic 411 outage (Rich Mintz)

On 25 Nov 1996, Bell Atlantic (the local telephone company serving the mid-Atlantic region of the USA, including Philadelphia and Washington, D.C.) had an outage of several hours in its telephone directory assistance service, due apparently to an errant operating-system upgrade on a database server. For unknown reasons, the backup system also failed. The result was that for several hours telephone operators ended up taking callers' requests and telephone numbers, looking up the requested information in printed directories, and calling the callers back with the information. Apparently, the problem was solved by backing out the software upgrade. Significantly (in my opinion), *The Washington Post*'s article on the outage mentioned this fact (albeit in slightly less technical language), which is yet another indication of the pervasiveness of software, and of the growing number of people in society at large that are generally aware of software and how it works.

[Christopher Palermo (R 18 64) noted that Northern Telecom said that the new upgrade was intended to correct some minor errors in the earlier version, and had previously been used without incident by at least two other large telcos. Blame was allocated to a technician who had installed the software. This was reportedly one of the biggest outages of this kind ever. Robert J. Perillo added (R 18 65) that about 60% of BA's 2000 operators at 36 sites could not access their directory system, affecting hundreds of thousands of customers in nine eastern states – apparently the most extensive such failure since operators began using computerized directory assistance. PGN]

Blown Fuse Takes Out 911 System (Scott Lucero)

National Public Radio reports that a blown fuse took out a large portion of Iowa's 911 emergency phone system for three hours over the Thanksgiving weekend. U.S. West could not say how many 911 calls went unanswered. A spokesperson said that the troubles isolating the problem came from the complexity of the system. The RISKS are pretty evident.

Tote Board Crash at Breeder's Cup (Tony Harminc)

The Breeder's Cup – an American horse race being run for the first time in Toronto on 26 Oct 1996 – suffered from various organizational difficulties, according to an article in the Toronto *Globe&Mail* on 28 Oct 1996. Among these was that the "tote board" – the display of current betting odds – crashed. "Betting was never halted during the tote board disruption, but [Ontario Jockey Club president David] Willmot said it probably cost about [CA]$400,000 in local betting handle because serious players will not make large bets unless they can see exact odds. It was a $35,000 bet in US currency that crashed the system. The software designed to convert US money to Canadian in the tote pools could not handle such a large amount." [Hmmm... $35,000. Do you suppose a bet of oh, say $32,767 might have worked? TH] [See (R 18 58,60) for followups. PGN]

1996 Melbourne Cup off-course betting fiasco (Harley Mackenzie)

The Melbourne cup is Australia's premier horse race (handicap over 3200 metres with over $AUS 2 million prize money), that even has its own public holiday in metropolitan Melbourne. The whole nation stops to listen or watch the race and many once-a-year punters have a dabble on the cup. The TAB (used to stand for Totaliser Agency Board when it was government owned and run, but it is now a public company) is the *only* (legal) provider of off-course racing betting in Victoria. However, when the punters turned up at their local TAB (or pub TAB located in hotels) to place their bets on yesterday's race (5 November 1996), there were queues that stretched out the door for hundreds of meters. The 15-year-old computer system had failed again on Melbourne Cup day, and most small agencies were off-line from about 10:45 am (AESST) to just before or after the running of the cup at 3:20pm (AESST), whilst the larger agencies were off and on with reduced numbers of active windows throughout this period. ... It is difficult to understand how the TAB system could not be designed and tested to accommodate the peak betting activity; the Melbourne Cup *always* results in this level of high activity, and is therefore predictable and – you would imagine – able to be simulated. [See R 18 58 for the rest of the story.]

Data diddling in cockroach races (David Kennedy)

A well-organised criminal group that made more than 800 million roubles every month by manipulating computer files in gambling has been exposed by police in the Saratov region of Russia, in the middle Volga. A source in the regional directorate in charge of fighting organised crime told Itar-Tass that computer-added swindling was exposed by police for the first time in Russia, although crimes of this sort have been reported in many regions of Russia. The source described the technology of fraud: the operator used a false file to influence the outcome of the "cockroach races" in a way that ensured that the victory was won by the cockroach chosen by the operator. (The net take was about US$5,500 daily.) [Source: Criminal group made money by manipulating ..., Itar-Tass, COMTEX Newswire, 25 Nov 1996] [Perhaps the swindlers were singing, Nobody knows the roubles I have seen. PGN]

Instant money (Debora Weber-Wulff)

A soldier is under investigation after allegedly transferring more than a half-million dollars into his checking account from his savings account. The problem was, it wasn't his money. On 29 Nov 1996, he unsuccessfully attempted to withdraw money from his overdrawn accounts. Then he conducted a transfer of $600,000.21 from his savings to his checking account at an ATM (banks were closed for the day after Thanksgiving). Because of a defect in the ATM computer system, the transfer was completed without verification of whether funds were available in the soldier's account. Over the next few days, the soldier was able to withdraw $300 in cash and deposited $30,005 into a newly opened credit union savings/money-market account. On 2 Dec he attempted to wire $60,000.15 to California. Officials noticed the error and stopped the transaction. The soldier was apprehended, but

has not been charged and is not in custody.

A spokeswoman for the bank said the incident was the result of a one-time glitch in the bank's computer system. An anonymous customer service representative said there have been problems with the bank's computer accounting system since 8 Nov 1996 – the day the data from Bank A was converted to Bank B. [The military awards its banking contracts only for a limited duration. They have problems at every change-over, it seems.] "From that point on, we've just been trying to fix messes," the bank employee said, noting that the problems range from lost data to false duplication. [Source: *Stars & Stripes,* 7 Dec 1996. Excerpted by DWW.]

Another banking system hits the dust (John C. Bauer)

On 30 Nov 1996, the Canadian Imperial Bank of Commerce Interac service was victimized by its attempted software upgrade, affecting about half of all would-be transactions across eastern Canada. [Source: Debit card failure angers customers, by Colin Freeze, Citizen Correspondent, *The Ottawa Citizen,* 2 December 1996, Ottawa, Ontario, Canada. PGN Stark Abstracting] One business affected was Loblaw's, a grocery chain. Grocery stores do not accept credit cards. (My wife Ann says it may a provincial law.) I can just see someone with a cartful of groceries arriving at the checkout and being asked for cash they are not carrying. As of 1 p.m. EST, 2 Dec 1996, the local branch of the bank had no statement to give to customers! Will this be touted as another example of computer people living outside the real world, where shopping is at a peak on Saturday afternoons, especially near Christmas?

Fidelity Brokerage computer problems (George C. Kaplan)

An article in the *Wall Street Journal,* 4 Nov 1996 describes a major problem for Fidelity Brokerage Services (a discount stock brokerage) in London. Very few details are given beyond "late bookings of dividends and other problems", but it's serious enough that more than 50 people are working 14-hour days to sort through and correct three months of records *manually.* British authorities have forced FBS to stop taking new customers until the problems are solved. This appears to be a familiar story to RISKS readers: A new system was rushed into operation in April without adequate testing. FBS seems to be in denial, claiming that the system wasn't rushed, but that they simply "ran into some unanticipated glitches."

Czech hackers allegedly rob banks (Mich Kabay)

Hackers stole 50 million Kc ($1.9 million) during attacks upon unnamed Czech banks and, in another incident, obtained and posted to BBSs a file of Czech citizens' personal information, according to an interview at INVEX (Brno, 22-26 Oct 1996) with Jiri Mrnustik, CEO of the Brno-based anti-virus and encryption software developer AEC s.r.o. [Source: Secret incidents of hackers' attacks upon Czech banks and release of Czech citizens' personal information, by Steven Slatem, Copyright (c) 1996 IntelliTech, from the on-line "Central & East European Secure Systems Strategies (CEESSS)", with permission.]

ATM problems in Canada (Richard Akerman)

Toronto-Dominion bank's automated teller machines crashed for most of the weekend, affecting the bank's 2000 machines. The TD debit payment system was also down. In Canada, 80% of the banking is done electronically, and the 30 million residents have 43 million bank cards. In a separate item, some Royal Bank customers had their accounts debited but received no cash. [There were 1.023 billion ATM transactions in 1995 (about 35 transactions per year for every person in Canada).] [Source: Halifax *Daily News,* 29 Oct 1996, p. 19. Reported in Canada by Rob Ferguson, The Canadian Press (CP) agency, in many papers. PGN Abstracting.]

Mars Probe crashes (Ben Morphett)

When the Russian Mars probe crashed in mid-November 1996, it provided an interesting example of the difference between precision and accuracy. The first reports said that the probe would crash land in central Australia, bringing with it 200 g of plutonium. State emergency services all over Australia went into yellow alert. Soldiers were mobilised. From the TV pictures, the first estimates of where it would land were anywhere in an area about 2000 km across. The next reports said that it would be landing at about the New South Wales/Queensland border, and they seemed to think it would come down somewhere in an area about 500 km across. The next reports said that it would come down somewhere in an area in the north west of New South Wales, and the precision of this estimate seemed to be about 100 km.

As it turned out, it came down about 2000 km west of Chile, in the Pacific Ocean, a third of the way around the world from Australia. So as the precision of the reports was increasing, the accuracy of the reports was about staying about the same – very wrong.

More on the Aeroperu crash (PGN)

Investigators of the Aeroperu crash (RISKS-18.51) are considering whether some of the plane's sensor ports ("static ports") might have been left with protective duct tape covering them when the plane took off. (*San Francisco Chronicle,* CNN, etc.) It is apparently normal maintenance procedure to cover the ports (marking them with bright "Remove Before Flight" markers), to prevent them from getting clogged. For further analysis, see Peter Ladkin (R 18 59).

Cruise Missile software bugs (Kofi Crentsil)

I don't remember seeing anything in RISKS on software bugs deflating the success rates of recent cruise missile strikes on Iraq. It all sounds very similar to the Ariane-5 software reuse fiasco. Here are some relevant excerpts from David A. Fulghum's "Hard Lessons in Iraq Lead to New Attack Plan" in *Aviation Week & Space Technology,* 16 Sep 1996, pp. 24-25. "Bomb damage assessment of the initial cruise missile strike indicates that three of the 10 targets attacked by 13 Air Force CALCMs (Conventional Air-Launched Cruise Missiles) emerged with 'no detectable damage,' according to a U.S. intelligence report. The Boeing built CALCMs, converted from Cold War-era nuclear weapons at a cost of $165,000 each, were

launched from two B-52H bombers over the Persian Gulf." ... "Part of the problem with the CALCMs were that they were fired at targets they were not designed to destroy, a product of hasty planning, according to a senior Pentagon official. Air Force success rates were further deflated because of missile computer programming quirks." ... "Another CALCM target escaped damage because of a software targetting quirk left over from its nuclear role. If two CALCMs are aimed at the same target at the same time, one of the missiles will re-aim itself at the next highest priority target. In the initial raid, one CALCM missed the target while the other went on to the next site." The risks of reusing software without proper testing for the new application are obvious.

"Software explosion rattles car makers" (Daniel P. B. Smith)

Automakers are facing runaway growth in the lines of code their engineers must write and manage as microprocessors take over automotive functions. "Software is where the problem is today," said William Powers, VP of research at Ford. "Today, if you change a line of code, you're looking at the potential for some major problems. Hardware is very predictable, very repeatable. Software is in much more of a transient state." The volume of code is exploding as processors proliferate behind the dashboard and under the hood. The typical auto has 10 to 15 processors; high-end cars can have as many as 80 ... "An engine controller can have 100,000 lines of code" [according to a Bosch VP]. [*Electronic Engineering Times,* 28 Oct 1996, front page.]

Lawyers eager for millennium cases (Stayton)

Lawyers eager for millennium cases: The year 2000 glitch that may trip up computer calendars could bring a slew of lawsuits, by Christian Plumb, Bloomberg Business News, *News & Observer,* Raleigh, NC, Sunday, 3 Nov 1996, page 5F: "It's just a gold mine." "It's like a law-school case of tort issues." [Charles R. Merrill, of McCarter & English, Newark, NJ.] Perhaps IT managers will take better notice of the Y2K problem – if lawyers start getting on their case.

ONE-LINERS:

- Communications errors delay response to San Francisco fire (R 18 68)
- Three awards (largest $5.3M) for arm, wrist, hand injuries attributed to Digital LK201 keyboard (S 18 66); references on RSI (R 18 68)
- Van Nuys CA doughnut shop turns up in LAPD database because it is closest address to high-crime mini-mall street (R 18 70)
- More on the accidental F-15 shootdown during training mission (R 18 57)
- Complexity of the airplane pilot's interface increasing (R 18 63)
- Computer errors involved in plane crashes? (Aftonbladet) (R 18 65,66)
- Problems with below-sea-level aircraft altitudes (R 18 72,74)
- Risk of snowbound east-coast bookstore phones forwarded west (R 18 65)
- AOL enables blocking of 53 domains in attempt to reduce junkmail (R 18 56,62)
- Connecticut Dept of Public Utility Control gets slammed (long-distance carrier changed) (R 18 69)
- More ghost phone 911 calls resulting from phone system changes (R 18 71,72) and related number compatibility issues (R 18 72).
- Risk of 16-bit MIS-Access installed on WFW or Windows 3.1 (R 18 65)
- Risks of PC changes without changed model numbers (R 18 70,71)
- WinWord 6 "feature" and discussions of compatibility problems (R 18 70,71,72)
- More Y2K problems: Visa credit-card expiration-date problem (R 19 62,65); legal liabilities (R 18 63)
- More on cleaning person inadvertently killing patients (R 18.29,29): story later debunked (R 18 72)
- More on -32768 (R 18.55,57,58,60,61)
- More on Denver airport: city overruled consultant's simulations (R 18 66)

SECURITY AND PRIVACY

Major denial-of-service attack on WebCom in San Francisco Bay Area (PGN)

A 200-message-per-second SYN-flood attack (see S 22 1, R 18 45 for the precursor PANIX attack, and R 18 48 for some defenses) was launched against WebCom (a large WWW service provider), affecting more than 3000 Web sites for 40 hours during most of what was otherwise a very busy shopping weekend. The attack began Saturday morning, 14 Dec 1996 shortly after midnight PST. (See R 18 69 for some details.) [Source: High-Tech Attack Shuts Down Web Provider in Santa Cruz, an AP item written by but not attributed to Elizabeth Weise, seen in the *San Francisco Chronicle,* 17 Dec 1996, C18. PGN Stark Abstracting]

U.S. Air Force webpage hacked (PGN)

U.S. Air Force has now joined the club along with the Department of Justice, CIA, and NASA, whose webpages had previously been altered by intruders (RISKS-18.35 and 49). On Sunday morning, 29 Dec 1996, the main webpage of the Air Force's website http://www.af.mil at Fort Belvoir, Virginia, included various antiGovernment slogans, plus a suggestive graphic of what the Government is doing to you (R 18 74). [Source: Hackers Disrupt Air Force Web Page, article by Seth Schiesel, *The New York Times,* 30 Dec 1996.]

Reuters computer tech brings down trading net (Steve L)

Dealing rooms sabotaged by HK Reuters technician, By Nicholas Denton in London and John Ridding in Hong Kong, 29 Nov 1996 Financial Times Limited

A disgruntled computer technician at Reuters in Hong Kong has caused the financial-information provider deep embarrassment by sabotaging the dealing-room systems of five of the company's investment bank clients. The attack crippled for

up to 36 hours the computer systems bringing market prices and news to traders at NatWest Markets, Jardine Fleming, Standard Chartered, and two other banks. The banks, which resorted to alternative terminals such as Bloomberg, claimed the tampering had no significant impact on trading and said neither they nor their clients had experienced losses as a result.

The incident was reportedly the most serious breach of security disclosed in Reuters' corporate history, and is causing some rethinking of privileges. The maintenance engineer in question has been suspended. He apparently visited the client sites and initiated deferred commands to subsequently delete specific operating system files.

ATM Fraud in Israel - The Polish Gang (Jonathan Rosenne)

A judge in Tel Aviv has ordered the remand in custody of two additional suspects in a major ATM fraud case, who will join five businessmen from Poland. The gang are suspected of having prepared thousands of counterfeit ATM cards. The police claim they had purchased tens of thousands blank plastic cards in Greece, on which they recorded the magnetic stripe and on each there was a sticker with the PIN. A Israeli computer expert, Daniel Cohen of Ramat Gan, also in custody, obtained the codes and manufactured the cards. The Polish businessmen financed the operation, and planned to bring foreign workers from Poland to use the cards to withdraw money from ATMs. The police have photographs of suspects standing next to ATMs holding quantities of forged cards. They had used them to withdraw 1,500 Israeli Sheqels (500 US Dollars) each, to a total of IS 600,000 (US$200,000). [Source: Yediot Aharonot, October 23, 1996]

Massive NY City tax fraud(Mich Kabay)

New York City workers, in exchange for bribes from property owners, falsified computer records to eliminate nearly $13 million in unpaid taxes in a scheme called the largest tax fraud case in New York City history. The author makes the following key points: Some tax records were erased. Other records were falsely marked as paid using funds from legitimate payments by innocent victims. So far, 29 people have been charged in federal court. 200 more are expected to be charged. $13M of debts have been erased. $7M in interest was lost. The fraud is thought to have started in 1992. The investigation started in 1994. In a section particularly intriguing for RISKS participants, the author writes, "Three employees of the city collector's offices exploited computer "glitches" to make it appear that unpaid taxes had been paid, officials said. [Source: Hacker Scheme, By Karen Matthews, Associated Press news wire via CompuServe's Executive News Service, AP US & World, 22 Nov 1996]

ONE-LINERS:

- Plot to tap British bank/credit card information by higher-tech gang revealed by coerced software expert in jail (R 18 70)
- New York Yankee World Series victory parade; in absence of stock-market ticker tape, confidential records from NYC Housing Authority and Dept of Social Services rained down (R 18 55)
- Palisades Park NJ school employs 16-yr-old to break into locked-up computer system – need for key recovery mechanisms? (R 18 70,71)
- Visa victim of PC theft with info on 314,000 credit-card accounts (R 18 62)
- Nasty scam exploiting Y2K authorization expirations (R 18 68)
- Intel LANDesk Manager reaches directly into networked workstations (R 18 59)
- Microsoft Java/COM integration support does automatic upgrades (R 18 64)
- China strengthens control over "cultural rubbish" on the Internet (R 18 73)
- Danish government puts its own records on the Web, illegally (R 18 63)
- Irish rock band U2 unreleased songs pirated from demo video, distributed on the Internet (R 18 62,63)
- Making good ActiveX controls do bad things (R 18 61); more risks (R 18 62)
- Good Java security vs good network security (R 18 61)
- NT passwords bypassable by overwriting hashed password (R 18 62)
- More on crypto attacks: Research note from J.-J. Quisquater on crypto fault analysis (R 18 55); more from Adi Shamir on differential fault analysis (R 18 56) and Paul Kocher (R 18 57); Ross Anderson (R 18 58); role of replication? (R 18 58); history – note on Bletchley Park Colossus breaking Fish ciphers (R 18 59); practical tampering attacks, Ross Anderson and Markus Kuhn, Usenix Electronic Commerce paper (R 18 62); more from Quisquater (R 18 64)
- Why cryptography is harder than it looks, Bruce Schneier (R 19 61)
- Cryptography Policy and the Information Economy, Matt Blaze (R 19 71)
- Security flaw in NCSA httpd phf (R 18 69,70); CERN httpd (R 18 71)
- Risks of CT fingerprinting system to catch welfare recipients (R 18 69)
- German Cabinet approves Internet privacy, censorship regulation (R 18 69)
- Justice Dept wants to scrutinize parolee computer use (R 18 70)
- More on cookies (R 18 63,65,67,68,70,72); residues in Internet Explorer 3 (R 18 68); ActiveX security risks (R 18 69)
- Residue problem in frequent-flier miles on number reissue (R 18 65)
- Interference effects of the next cycle of solar activity (R 18 62,63)
- U.S. program export controls ruled unconstitutional by Northern California federal judge, Marilyn Hall Patel (R 18 69)