The INFOSEC Year in Review: 1996

M. E. Kabay, PhD, CISSP
Security Leader, INFOSEC Group, AtomicTangerine, Inc.

Human beings like perspective. Maybe that's why every year, so many of us like to look back over the last 12 months in our respective fields and remind ourselves of what's changed. The NCSA NEWS publishes The InfoSec Year in Review" to make sense out of information security news; our Research, Education and Consulting Group at NCSA naturally gets the pleasure of writing the review. The following version is much expanded over the original report published in the January 1997 issue of NCSA NEWS and is kept up-to-date month by month for the InfoSec Update course. Herewith, some thoughts on some of the most interesting issues in InfoSec in this past year.

January 1996

A problem occurred in the very first second of the year: the addition of a leap second caused problems with software controlling the broadcast of Coordinated Universal Time from the National Institute of Standards and Technology (NIST). The extra second caused a whole day to be added to the date [RISKS DIGEST 17.59]. Watch out for the year 2000 (Y2K) if you want to see real problems with calendars and clocks.

From early January through the end of February, Worldwide negative comments continued about CompuServe's end-of-1995 banning of 200 USENET groups in a wild over-reaction to Bavarian prosecutor's request for information about their availability of groups which might be illegal in a southern province of Germany. CompuServe, unable to bar access to the groups for a subset of its users, barred access for all 4 million subscribers around the world. By the end of February, access was barred for the geographical location in question. The irony of the ban is that there are well known methods for accessing USENET groups via e-mail. The wider implications of this story include the growing tendency to impose local (provincial, state, national) restrictions on access to parts of the Internet [see RISKS 17.59 ff for more details].

The Wall Street Journal reported early in the year that the first court-authorized wiretap of a commercial Internet Service Provider had resulted in the arrest of three individuals alleged to be running a cell-fraud operation advertized through CompuServe [Wall Street Journal*, 2 Jan 1996, p.16 via EDUPAGE].

On January 22, German television showed a member of the Chaos Computer Club demonstrating the perils of cleartext transmission of personal banking information through T-Online. The hacker (not a criminal hacker, by the way) tapped into a home telephone line by clipping into the unlocked panel in the basement of an apartment building and captured the user's ID and PIN. He then interrupted the call and immediately transferred 5,000 DM into another account. Before making the demonstration public, the Chaos Computer Club had warned the banking industry and consumers to insist on encrypting data transfers throughout the entire financial system's communications networks, starting at the desktop. [RISKS 17.66 ff]. By the way, I have met one of the principal members of the Chaos Computer Club, Andy Müller-Maguhn, and have been impressed by his apparent commitment to non-criminal hacking. I wish more criminal hackers would see the light and behave in a responsible, civic-minded way as the CCC seem to be doing.

Matt Blaze, Whitfield Diffie, Ronald L. Rivest, Bruce Schneier, Tsutomu Shimomura, Eric Thompson, and Michael Wiener published their paper, "Minimal Key Lengths for Symmetric Ciphers to Provide Adequate Commercial Security." The authors proposed that 40-bit keyspaces for symmetric encryption are no longer adequate to prevent brute-force attacks and even 56-bit keys are now effectively untrustworthy. They strongly recommend a minimum of 75 bits for today's keys and at least 90 bits to protect against advances in computer power in the next 20 years. A PostScript copy of the full text of the report is available in ftp://ftp.research.att.com/dist/mab/keylength.ps
The file ftp://ftp.research.att.com/dist/mab/keylength.txt contains an ASCII version.

And from the NCSA's IS/Recon group, a few more tid-bits:

In the Netherlands, a political scandal erupted over accusations of eavesdropping in a major bank. Employees were monitored for performance without their awareness or permission.

Russian citizen Alexei Lachmanov, pleaded guilty to charges of participating in the $2.8 million Citibank wire fraud masterminded by St. Petersburg mathematician and criminal hacker Vladimir Levin.

Dan Farmer, author of the Internet-security testing program called SATAN, released a new utility for comparing operating systems against the standard versions (thus helping to identify patches and possible Trojan Horse software). Typically, he called his new program "FUCK." Presumably, no on one AOL will be allowed to refer to this new program by name (thanks to their automated obscenity filter)....

The Association of British Insurers released a report estimating that computer crime is costing about 1 billion pounds a year in damages to industry.

Barry Jaspan located a bug in the security shell "ssh" which allows users to retrieve an RSA secret key from memory, thus compromising the entire host-based security system. The discovery took 20 minutes, leading the security expert to wonder how many other bugs in ssh remain to be discovered with a little more work.

Lotus Notes announced that it would now include an escrowed key permitting the U.S. government to decrypt any encrypted information in the groupware product. Privacy advocates warned that this was an end-run around the opposition to the Administration's Key Escrow proposal, which has been poorly received by industry.

MCI announced that it would henceforth close the accounts of anyone spamming the Net (i.e., sending high-volume unsolicited e-mail or filling news groups with inappropriate messages). Observers wondered who would decide which messages offend these ill-defined rules.

February

On February 14, the New China News Agency reported that all users of the Internet in China would henceforth have to register with authorities. This marked the beginning of the formal process of locking up Internet access in the People's Republic of China; in September, China blocked access to over a hundred Web sites, including The Wall Street Journal, the Washington Post and CNN. By the end of 1996, Chinese users were officially limited to what is in effect an Intranet, with all traffic limited to what passes through the national firewalls.

A rash of stories appeared in the non-technical news media about the supposed danger of infection by a Windows95-specific virus called Boza/Bizatch. Early comments by experts about the extremely low probability of being hit by this virus were removed as the stories ground through the news wire rumor mill, resulting in a panic among unsophisticated PC users and general but unwarranted discredit to the anti-virus industry.

A federal judge in Philadelphia issued a partial temporary restraining order prohibiting enforcement of the "indecency" provision of the Communications Decency Act (CDA). This was the first victory in a legal battle against the constitutionality of the CDA, passed in late 1995 and generally reviled because of its putative violation of the First Amendment of the United States Constitution barring prior restraint on speech. [For detail about this case and the eventual success in barring enforcement of the CDA, see http://www.epic.org and http://www.aclu.org/issues/cyber/trial/trial.htm] The case moved to the Supreme Court calendar in December and arguments will be heard in March 97.

Intuit Inc. admitted that some of the calculations were wrong in its US tax-preparation software, TurboTax and MacInTax. The company scrambled to post updates on its Web site, offered workarounds, and promised to pay penalties imposed on its customers because of its program's errors. This case is useful for all teachers and practitioners of quality assurance when trying to illustrate the cost and benefits of investing more than half the total software development efforts into QA.

Professor Ed Felten and his graduate students at Princeton University continued their analysis of JAVA security weaknesses. [Seehttp://www.cs.princeton.edu/sip/ for details.] In November, David Martin <dm@cs.bu.edu> of Boston University and his colleagues Sivaramakrishnan Rajagopalan <sraj@bellcore.com> and Avi Rubin

<rubin@bellcore.com>, both from Bellcore, pointed out [in RISKS 18.61] that JAVA applets can attack firewalls from the inside. [See their paper at http://lite.ncstrl.org:3803/Dienst/UI/2.0/Describe/ncstrl.bu_cs%2f96-026]

Peter Neumann, moderator of RISKS, reported on another cybervandalism case as follows in RISKS 17.83 (remarks in square brackets are MK's, not PN's]:

> BerkshireNet in Pittsfield, Massachusetts, was the victim of an attack on 27 February 1996 in which someone planted swastikas and racist messages while masquerading as the provider's administrator, erased data on two computers, and then shut down the system. It was off the air for about 12 hours. Older deleted files were restored, but files created in the last several days were lost.... [Yet another case illustrating the importance of (a) protecting one's Web site against unauthorized modifications; and (b) the value of appropriately frequent backups.]

On February 29, reported a correspondent in RISKS 17.81, there were six different interpretations of the date in messages sent from different systems to his e-mail in-tray: 29 Feb 96, 28 Feb 96, 1 May 131, 10 Jan 1936, 1 Jan 70 and 29 Dec 95. Yet another brick in the Y2K wall . . . .

> In England, criminal hackers altered the announcements of talking bus stops [RISKS 17.81]. In a demonstration of their much-vaunted position that criminal hacking is a form of useful social protest (see any issue of ***2600, The Hacker Quarterly*** for this kind of pap), the cybervandals replaced information of use to blind people by curses and obscenities.

> IS/Recon staff added that a lengthy post in February attributed to Nathaniel Bornstein claimed that "First Virtual Holdings has developed and demonstrated a program which completely undermines the security of every known credit-card encryption mechanism for Internet commerce." The post suggested that the problem cannot be fixed with a patch, that it is fundamental flaw in all credit card encryption schemes. The author suggested in strong terms that all methods of passing credit card information are inherently insecure [because the keystrokes of personal computers can be recorded with Trojan software]. He stated: "on personal computers, INFORMATION IS INSECURE THE MOMENT YOU TOUCH A KEY"

March

In early March, the White House e-mail system was flooded with fraudulently-requested, unwanted subscriptions to Internet mail-lists. The autoresponder at whitehouse.gov responded to the incoming automated e-mail by sending out responses to the lists, causing additional congestion on the Net. This denial-of-service attack is just one example of a major and growing problem in cyberspace. In this case, the problem occurred because it's easy to forge e-mail headers and many (or maybe most) mailing-list software cannot identify fraudulent requests for subscription.

The PKZ300B.ZIP or PKZ300.EXE Trojan Horse continued to break into news in March. Do not download, upload, transmit or execute files claiming to be a PKZip version 3.0: these two are imposters that can wipe out hard drives. The latest version of PKZip is 2.04g; filename is supposed to be PKZ204g.zip.

From EDUPAGE:

> Legislation has been introduced in both the House and Senate to permit the export of data encryption hardware and software if similar technology is available from foreign suppliers. The bills affirm the right of U.S. citizens to use any type of encryption equipment domestically, and prohibit the mandatory use of special keys that would allow law enforcement officials access to encrypted messages. In addition, the legislation would make it a crime to use encryption technology in the commission of a crime. (*The New York Times*, 4 Mar 1996, C6)

According to the New York Times (7 Mar 96), a letter intended to go to 89 credit-card customers to let them know their accounts were in default went to 11,000 (of a total of 13,000) customers using Chase Manhattan's secured credit-cards. [Ironic that the software glitch resulted in annoying most of the most trustworthy (and richest) people in the client base. How about another point in support of better QA?]

In Australia, The Sunday Mail in Queensland (Mar 10) reported on the interesting case of the two Belindas: both women are named Belinda Lee Perry and both were born on 7 January 1969. Because of poor choices by computer programmers and analysts in defining supposedly unique identifiers for people, the identical names and birth dates

guarantee a lifetime of confusion for these women. On various occasions, each has had her own information over-written by the others, causing endless trouble. The one positive note is that these ladies have now become friends. [Surely program designers ought to realize by now that name x birth date is an inadequate "unique" identifier?]

EDUPAGE reported that the Federal Trade Commission (FTC) has begun a major attack on Internet- and Web-based fraud. According to Investor's Business Daily (15 Mar), the FTC filed charges against nine individuals and companies accused of fraudulent misrepresentation.

The Wall Street Journal (15 Mar) [via EDUPAGE] reported on claims by a manufacturer of disk drives, IOMEGA, that false information posted on the "Motley Fool" section of America Online was causing irregularities in trading of its stock. The company complained to the Securities and Exchange Commission. Analysts pointed out that it is foolish to place any trust in anonymous or pseudonymous postings of this sort. [Caveat lector!]

The Computer Incident Advisory Capability (CIAC) of the US Department of Energy issued its CIAC Notes Number 96-01 on 18 March; the lead article summarized the status of Java and JavaScript security bugs and fixes. [See http://ciac.llnl.gov/ for archives.]

Our own David Kennedy reported (in RISKS 17.95) that at the end of March, authorities in Argentina arrested Julio Cesar Ardita, 21, of Buenos Aires, sysop of The Scream BBS and better known as "El Griton" in the computer underground. He was accused of systematic and major unauthorized intrusions into systems at Harvard, the U.S. Navy, NASA computers, U.Mass, CalTech, Northeastern U and also computer systems in Brazil, Chile, Korea, Mexico and Taiwan. One of the interesting aspects of the case is that the Harvard team used artificial-intelligence programs to sift through the thousands of possible user IDs to narrow the possible perpetrators down to a single ID based on his "computer habits." Government officials in Argentina seized his computer and modem in January. Despite close cooperation between authorities in Argentina and the US, the man was released without charge because Argentina has no law criminalizing unauthorized intrusion in computer systems. in addition, because of the requirement for "dual criminality" in international law, it was not possible for Argentinian authorities to extradite Ardita to the United States (the requirement states that an action must be defined as criminal in both countries before a person can be extradited). [This case illustrates the future of international computer intrusions in the absence of global--or even of bilateral--agreements on what constitutes a computer crime.]

Also in March, "U4ea," self-titled "darkside hacker," began a reign of Internet terror in the city of Boston, MA. This criminal hacker brought down BerkshireNet and a local ISP for 12 hours. In retaliation for articles about him, U4ea then attacked *The Boston Globe* computers and deleted their WWW pages and those at www.boston.net.

April

In early April, 19-year-old Christopher Schanot, known as "N00gz" in the computer underground, of St Louis was indicted in Philadelphia on computer fraud charges. This high-school honor student was accused of unauthorized access to many corporate and government computers including some at Southwestern Bell, BELLCORE, Sprint, and SRI. In November, he pleaded guilty to two counts of computer fraud and one count of illegal wiretapping. He faces up to 15 years in prison and $750,000 in fines at his sentencing on January 31, 1997. [AP 15 Nov]

Employees of the US Social Security Administration were revealed in news reports [see RISKS 18.02] to have misused their authorized access to SSA computers and sold detailed personal information about more than 11,000 victims to a ring of credit-card fraudsters. [Another lesson about the importance of human factors in security.]

Associated Press (19 Apr) reported that the New York Police Department's voice-mail system had been hacked; vandals replaced the usual polite announcements with "You have reached the New York City Police Department. For any real emergencies, dial 119. Anyone else -- we're a little busy right now eating some donuts and having coffee." It continued ``You can just hold the line. We'll get back to you. We're a little slow, if you know what I mean. Thank you." The bogus messages continued for 12 hours before they were corrected by officials.

Peter Neumann summarized a news article about an important development in the battle against the International Traffic in Arms Regulations (ITAR):

> U.S. District Judge Marilyn Hall Patel released a ruling on 16 April 1996 that mathematician Daniel Bernstein could try to prove that the U.S. export controls on encryption technology are too broad and violate his right to communicate with other scientists and computer buffs -- a right protected by freedom of speech. (Bernstein's cryptographic programs are called Snuffle and Unsnuffle. The U.S. State Department decided in 1993 that Bernstein's written article and programs required export licenses [because crypto purveyors are considered as being international arms dealers under ITAR], but later backed down on restricting the article; Bernstein then had sued for release of the programs.)

In December, Judge Patel struck down the ban, describing it as a "paradigm of standardless discretion" that failed to protect citizens' free speech rights. [UPI 19 Dec; RISKS 18.69]

According to the San Francisco Chronicle of 20 April [summarized by Peter Neumann in RISKS 18.07], the personal secretary of a Vice-President of Oracle Corporation received an out-of-court settlement after she sued for wrongful dismissal. She claimed to have been fired because she refused to copulate with the President of the company and provided as evidence a piece of e-mail that purported to be from her boss to the President confirming that he had fired her as the President had asked. However, investigation suggested that in fact, her boss was actually driving his car at the time the e-mail was sent (or so suggested his cellular phone records). The plaintiff also knew her boss's passwords (he used to ask her to change them for him). The local prosecutor came to the conclusion that she had fabricated the e-mail message and charged her with felony perjury. Peter Neumann's conclusions were interesting:

1. Don't believe e-mail FROM: headers accurately represent the sender.
2. Don't believe the content of e-mail, whether or not the headers are correct.
3. Don't share your passwords overtly with anyone, or let someone else be responsible for your passwords.
4. Don't use covertly compromisible reusable fixed passwords; how often you change them is more or less irrelevant.
5. Use one-time nonreusable authentication tokens instead of fixed passwords.
6. Even if you use PEM, PGP, stronger-crypto e-mail, or whatever, you cannot ensure authenticity, because of untrustworthy operating systems and untrustworthy users.
7. Beware of trying to use e-mail as nonrepudiatable court evidence.
8. HOWEVER, don't believe that cell-phone records are valid as court evidence; they too could be bogus or altered. If someone drags you into court, find someone who can demonstrate how easily those records could have been altered!

. . . to which Mike.Marler@oit.gatech.edu (Mike Marler) added [in RISKS 18.07],

9a. Don't believe that a person cannot have a batch job or background process running on their machine, which could send e-mail to another address (with or without "fudged headers"), while the person is, for example, 5 miles offshore of Costa Rica catching sailfish.
9b. Don't believe that a person cannot have an automated answering service that sends a reply to "a piece of e-mail" stating something similar to the following: "Sorry I cannot send a detailed reply to your 'piece of e-mail', because I will be very busy in meetings until the end of today". When the actual person is "playing hookey" or still chasing those sailfish in Costa Rica.

J.R.Valverde (jr)" <jrvalverde@samba.cnb.uam.es> added,

10. Never accept to handle the account of some other person or having access to his/her computer.

America Online caused hilarity on the Internet and in the British town of Scunthorpe when resident Doug Blackie tried to register his new account. According to an article in the Computer underground Digest (CuD) 8.29 [and summarized in RISKS 18.07], the indecency filter in the AOL program rejected "Scunthorpe" but accepted "Sconthorpe." The filter has ever since been known as "AOL's Scunthorpe Filter." In other RISKS postings, many people commented on the effects of exclusion of American slang on inoffensive words with false positives in English and especially in other languages. [One would think that the AOL programmers might have learned something from the design of recent anti-virus scanners.]

A report from the Daily Mail in England (27 Apr) [RISKS 18.09] stated that (a) criminal hacker(s) broke into confidential files at Cambridge University and led to emergency password changes for 10,000 students and staff. Some of the files included medical, commercial and academic information. Despite this spectacular report, however, the truth

was less glamorous: a posting from Stephen Early <sde1000@chiark.chu.cam.ac.uk> [RISKS 18.10] explained that a packet sniffer was found installed on a subnet of the University system.

May

A California legislator investigated why she was constantly receiving mail aimed at single parents. She found out that the algorithms implemented in state demographics programs included the assumption that if parental surnames on a birth certificate were different, the parents were not married to each other. The credibility of statistics such as, "30% of California mothers are single parents" is seriously weakened. In December, a similar furor erupted when USA Today published articles showing how the Computer Price Index definitions, rooted in an agricultural/industrial past, were wholly inadequate to measure productivity and costs in a post-industrial service/information economy. [GIGO, remember?]

According to EDUPAGE, DVD Software (Irvine, CA) produced a utility called UnGame that searches out and destroys computer games using a list that is updated monthly. More than 20 colleges and universities were using the software as of June to reduce time wasted by students taking up scarce terminals and workstations to play games while other students waited impatiently for computer access. (*Chronicle of Higher Education* 7 Jun 96, p. A24)

Installation of a new version of traffic-control software in Washington, DC inadvertently switched from the rush-hour stop-light pattern (50 seconds of green) to the weekend cycle (15 seconds of green). The resulting chaos doubled many people's commute time. [Washington Post (9 May)]

In France, the Internet Service Providers (ISPs) WorldNet and FranceNet chose to shut down access to all USENET groups because French prosecutors seized to hold the directors personally responsible for violating French national child-pornography laws. A storm of protest ensued, in which the AFPI (French Association of Internet Professionals) called for solidarity in blocking access to all of USENET in protest against the police action. [RISKS 18.11]

In a follow-up article [RISKS 18.13], simsong@vineyard.net (Simson L. Garfinkel) pointed out that blocking specific USENET groups that supply child pornography to pedophiles is relatively easy. Furthermore, he stated, storing or transmitting child pornography is a federal crime. In his opinion, "Any organization that has these news groups within the United States (including AOL) is in violation of federal law."

According to the AP news wire (18 May), the First National Bank of Chicago suffered the largest accounting error in financial history when a "computer glitch" [read "consequence of poor QA"] transferred about $900 million into each of about 800 accounts, resulting in a total miscalculation of $763.9 billion. [I wonder what _that_ programmer's bonus looked like this year?]

On May 18 also, the Australian Associated Press news wire reported that 55 computers were disemboweled (their RAM and hard drives stolen) in a state government building in Brisbane, Queensland.

The Jewish Publication Society issued a Jewish CD-ROM full of Judaica. Purchasers were startled and not too pleased when a Christian-oriented screen saver popped up. Seems the CD-ROM was created at a site that usually produces Christian stuff and the screen-saver was added in without thinking about the context. Happily for inter-faith relations, both parties admitted responsibility and are splitting the costs of re-pressing and redistributing a corrected version of the CD-ROM. [The person who summarized the case in RISKS 18.14, weemba@sagi.wistar.upenn.edu (Matthew P Wiener), joked that maybe the publishers had failed to provide adequate *beth*-testing.]

In Japan, reported the Wall Street Journal (22 May), a couple of Japanese Pachinko companies lost about U$588M when counterfeiters figured out how to counterfeit money cards and even how to refill them fraudulently. The electronic cash can be refunded to a bank account.

On 23 May, Rachel Polanskis <r.polanskis@nepean.uws.edu.au> reported that AltaVista had managed to index files in the root directory of an unsecured UNIX Web server. When she pointed at the URL with her browser, she found that she now had root access on a system she had never heard of before. She very kindly informed the site managers, who pulled the system off the Web at once for repairs to their security. Her conclusion was that poor security on a Web site is almost guaranteed to result in complete disclosure of and access to everything on the server. [RISKS 18.15]

An Associated Press new wire story summarized by David Kennedy in RISKS [18.15] reported on Senate testimony about computer security. The General Accounting Office (GAO) study based on the 1995 Department of Defense study of computer penetrations. The DoD estimated that there were about 160,000 attacks on unclassified military computers in 1995; their own Defense Information Systems Agency study using penetration attacks on 38,000 unclassified systems suggested that about 65% of all such attacks on unclassified systems would be expected to succeed but that only a tiny percentage would be noticed and even fewer would be reported appropriately to higher authorities in the military. Based on these studies, the GAO guessed that there might be something like 250,000 attacks on US government computers in a year. Other segments of the testimony suggested that about 120 countries are working on information warfare techniques. Peter Neumann added that the report is available from the Government Accounting Office as document GAO/AIMD-96-84, Information Security: Computer Attacks at Department of Defense Pose Increasing Risks.

The trade war between China and the United States heated up in late May when the US declared a $2B package of tariffs in retaliation for what it claims are massive, state-tolerated and even state-supported software-, music- and video-counterfeiting mills in southern China [Reuters 22 May]. Chinese bureaucrats countered that the US pressure against counterfeiting was actually a cover for what they termed "cultural infiltration."

In Israel, police shut down three pirate radio stations whose unauthorized emissions were scrambling wavelengths used by air-traffic controllers [AP 23 May]. The main airport in Tel Aviv was shut down in protest by the controllers. [If civilian radio stations can accidentally disrupt operations at a busy airport, what would high-energy radio-frequency devices (HERF guns) do?]
On the privacy front, a bill introduced to the US House of Representatives by Bob Franks (R - NJ) and to the Senate by Dianne Feinstein (D - CA) would bar disclosure of information about children without parental consent [AP 23 May]. Such information, collected by birthday clubs at supermarkets, toy stores, fast-food outlets and others, has been supplied to market research firms and direct-mail distributors. The bill's supporters argue that the mailing lists, which are available to anyone for a fee, are in effect lists of potential victims.

On May 28, Robert Alan Thomas, 40, of Milpitas, Calif., was sentenced to 26 months in federal prison and fined $50,000 by a judge in Utah for distributing child pornography. The sentence is being served concurrently with his prison term in Tennessee, in which he and his wife were sentenced to 32 months in Tennessee prisons for distributing obscene images of bestiality. [The legal implications of this case are very serious for operators of bulletin board systems; the judge ruled that each *download* of an image constitutes a basis for a separate prosecution.]

The National Research Council released its report on controls over cryptography at the end of the month. The panel of distinguished scientists strongly recommended removal of cryptography from the International Traffic in Arms Regulations and suggested that much of the purpose of restricting export of cryptography could be accomplished by developing cryptographic software that includes the possibility of key escrow or master keys to decrypt messages once a court order has been secured.

And from one of our underground research operatives, word that "Datastream Cowboy," a 16 year-old hacker from the United Kingdom, was arrested at his home and charged with breaking into Rome Laboratories Air Force base in New York and various other international computer networks. In another story, *9x* a Washington, DC-based criminal hacking group, begin releasing a series of hacking and phreaking text files.

June

The government of Vietnam promulgated new regulations to control access to the Internet and shut down any services deemed harmful to national interests. [AP 4 Jun]

The June 3 issue of the "London Times" reported that hackers had been paid 400 million pounds sterling in extortion money to keep quiet about having electronically invaded banks, brokerage firms and investment houses in London and New York with "logic bombs." According to the article, banks chose to give in to the blackmail over concerns that publicity about such attacks could damage consumer confidence in the security of their systems. [OTC 4 Jun]

News reports suggested that the Clinton administration would form a Cyber Security Assurance Group to work on defending the national interest against information warfare. [USA Today via AP 5 Jun]

In Pittsburgh, a three-year old received an income-tax refund check from the IRS for $219,495. The boy's parents had a hard time convincing IRS employees that there had been an error. ["But the computer says. . . ."]

At a hearing of the US Senate's Permanent Investigations Subcommittee, participants heard from Dan Gelber, the panel's chief minority counsel, that global losses in the commercial and financial services sector amount to $800M a year according to a survey by an unnamed research firm. More than half of these losses were attributed to U.S. companies. [Wall Street Journal, 6 Jun]

Keep those computers clean! A Swedish study reported evidence that the combination of dust plus static electricity results in higher rates of skin irritation for users of computer terminals. [RISKS 18.21]

Britain's Davy International initiated a lawsuit over industrial espionage against the Austrian firm VA Technologie AG; under court order, the plaintiffs received 2,000 pages of documents and computer disks containing information belonging to Davy International that were recovered from the defendants. VA Technologie vigorously contested the correctness of the charge. [Dow Jones 6 Jun] A few weeks later, Davy's parent company, the Norwegian ship-building firm Kvaerner ASA, joined the suit against VA. A few weeks later, VA Technologie filed a counter-suit against their accusers. [Dow Jones 21 Jun]

Chicago-area viewers of the familiar (and saccharine) game show, Jeopardy, were startled to find themselves suddenly watching cavorting, naked women rather than the usual three contestants phrasing answers in the form of a question. It seems that through some technical glitch, Continental Cablevision broadcast 10 minutes of the Playboy Channel in the slot assigned to the game show. [RISKS 18.22]

The Lexis-Nexis information service responded to an torrent of criticism, mostly from Internet users, by changing its P-Trak Person Locator Service so that it would no longer include the US Social Security Number. However, after receiving thousands of phone calls reacting to false information circulating on the Net, the beleaguered company offered ways to remove subject records from the database. [AP 13 Jun; UPI 20 Sep]

Attorney General Janet Reno supported key-escrow for strong cryptography but suggested that the escrow agencies could be private organizations rather than agencies of the US government.

The US Secret Service announced the arrest of 259 suspects accused of causing more than $7 million in losses from cellular phone fraud. [Reuters Jun 18] At about the same date, AT&T Wireless Services began a three-month public education campaign with posters in 570 New York City subway cars, on 200 interior poster cards on Staten Island Ferries and three billboards in Brooklyn. The posters warned potential thieves that cellular phone companies have the ability to track stolen phones.

In another case of alleged industrial espionage, the American subsidiary of Boehringer Mannheim Corp., a pharmaceutical firm based in Germany, accused Lifescan Inc., the diabetes-products division of Johnson & Johnson, of encouraging industrial espionage by presenting "Inspector Clouseau" and "Columbo" awards to employees who got the most information about their competitor. [AP 19 Jun]

Also in mid-June, the major Internet Service Provider NETCOM suffered a 13-hour service blackout that resulted in thousands of irritated customers and a dramatic fall in its share price from $33.25 to $28.75. [Reuters 21 Jun; RISKS 18.23] A day later, America Online Inc.'s e-mail system was knocked out for an hour when new software failed; quick-witted commentators immediately renamed the service "America Offline." In August, the AOL network went down for 19 hours.

In Britain, Mathew Bevan and Richard Pryce faced charges of conspiring to gain unauthorized access to computers and conspiracy to cause unauthorized modification to computers because of their alleged intrusions into computer systems operated by the US military and Lockheed missile and space company. [PA News 23 Jun]

Argentinian national Guillermo Gaede was sentenced to 33 months in federal prison by a Judge in San Francisco after admitting that he sent videotapes about Intel chip-manufacturing techniques to AMD, one of Intel's major competitors. AMD immediately notified police, leading to capture of the industrial spy. [Reuters 24 Jun]

CIA Director John Deutch warned Congress that the US faces a growing threat of cyberspace attacks against its computer networks by other nations and terrorists.

In Leonia, NJ, a 14-year old boy was arrested after using fraudulent credit card numbers to steal $5,000 of computer equipment. He was using a card-number generator program downloaded through the Internet and accidentally created the number of a credit card that had happened to have been reported stolen. [Reuters 29 Jun]

The June issue of *Health Letter* from the Public Citizen Health Research Group reports on the effects of radio-frequency interference (RFI) on medical devices. RFI has prevented apnea monitors from alerting staff when patients have stopped breathing; an implanted defibrillator delivered a shock to a normal heart; electrical devices have interfered with power wheelchairs; implanted heart pacemakers are particularly susceptible to RFI. [RISKS 18.47]

An item in the NCSA IS/Recon report for June was particularly interesting:

> **Library computer systems preferred "newbie" hacker target**
> Source: IS/Recon
> Date: 06/1996
> Confidence: high
>
> The IS/Recon team has observed that public library systems are a preferred targets for apprentice hackers. Use of these systems by "journeyman" hackers is also likely although we observe them proclaiming it less frequently than their juniors. Several IS/Recon underground sources recently published attack scripts used on the DYNIX flavor of UNIX that is used by many school and library systems in the U.S.
>
> After IS/Recon staff recently responded to the penetration of a small Internet service provider by a group of hackers, they discovered the group had thoroughly penetrated the public library network for that state. Another engagement we were working at the same time was an InfoSec evaluation of a company in that state. We discovered they have a terminal to the library network in the company's Learning Resource Center.
>
> IS/Recon staff recommends that any company with a public library network terminal isolate it with an "air gap" from the rest of its corporate networks.

July

Two people in Brooklyn were arrested for stealing 80,000 cellular phone numbers from passing motorists, the largest such heist in U.S. history, the Secret Service said. Had the numbers been sold on the black market, they would have been used to generate about $80M in stolen phone services. [AP 2 Jul]

The July 1996 issue of *Health Letter* reports that analog cell phones cause "minimal interference" 3% of the time but all digital phones caused some level of interference with cardiac pacemakers. [RISKS 18.47]

In a spectacular failure of cross-cultural quality assurance, Microsoft had to apologize for a Spanish-language electronic dictionary distributed in Mexico that provided offensive synonyms for many words and caused a political uproar. [6 Jul]

A 35 year old computer operator caused more than half a million pounds of damage to his employer, Thorn UK, by secretly disconnecting cables from their AS/400 minicomputer because of a grudge against his supervisor. Defense counsel argued that in addition, he had cracked under the strain of repeated back-to-back day and night shifts. The system went down repeatedly until an expensive specialist flown in from the US discovered the sabotage. He was sentenced to a year in jail. [PA News 9 Jul]

Police warned travelers to be on guard about laptop-computer thefts at airports. A common scenario involves a couple of thieves who watch for a victim to place his or her laptop on the X-ray conveyor belt. As soon as the computer is on

its way through the scanner, the two thieves squeeze into line in front of the owner; one gets through right away but the other, deliberately carrying lots of metal in his pockets, delays everyone for a few seconds. In the meantime, the first thief snatches the portable computer and disappears. [Wall Street Journal 9 Jul]

Windows Magazine reported in its August issue that many Web sites are unprotected against infiltration through ordinary browser programs. Using standard Web search-engines, the investigators discovered that many sites allow unrestricted read- and even write-access to file on the Web server. [See http://techweb.cmp.com/corporate for more details.]

The National Cable Television Association declared its intention to wire 95,000 private and public schools for high-speed access to the Internet. [AP 9 Jul] [There was no indication that the program includes any support for education of the children and teachers who will be using the Internet as a result of this ambitious program. Let's hope there's at least a baseline discussion of ethical issues before a new generation of criminal hackers develops out of ignorance.]

Singapore joined the list of governments trying to stem the tide of free information from elsewhere in the world. The new licensing strictly control Internet Service Providers; the rules force them to try to block anti-government views and pornography on the Internet, but authorities insisted they are not censoring anything: they're just asking licensees to exercise responsible behavior. [AP 11 Jul] Within a week, one of the suppliers blocked a USENET group where a Singaporean criticized a well-established Singapore law firm. [AP 19 Jul] The Chinese government's proxy server started operations in late August and was up and running in September. Burma banned modems and fax machines in late September.

High-school students in the San Francisco area broke into the PBX of a local manufacturing firm and attacked its voice-mail system. They erased information, changed passwords, created new accounts for their own use, and eventually crashed the system through overuse. The company spent $40,000 on technical support from an outside technician. [*San Francisco Chronicle* 10 Jul 96 p. A13 via RISKS 18.26]

In mid July, General Motors Corp. recalled 292,860 Pontiacs, Oldsmobiles and Buicks from the 1996 and 1997 model years because of an engine software problem that could result in a fire. [RISKS 18.25]

In Beijing, a student lost a precious $18,000 scholarship to the University of Michigan because her roommate signed onto their shared account and sent e-mail rejecting the scholarship in her name. [UPI 12 Jul] A month later, her roommate admitted her misdeed and paid a hefty fine. U Michigan re-accepted the applicant.

Dataquest announced projections that the worldwide information security market would double to $13.1B from this year's $5.9B by the year 2000.

The world's first known Excel macro virus, Laroux, was discovered in July, according to McAfee engineers. An anti-virus program was immediately made available by the company. The virus does not appear to include a harmful payload.

On 22 July, the Johannesburg stock exchange failed for the second time in the two weeks since installation on 10 July; cause: poor software quality assurance. [RISKS 18.28] In mid-October, the Cairo Bourse also experienced computer software problems in a newly installed-system; after the system crashed, stock prices and trading volume fell significantly. [Reuters 16 Oct] In December, the Hong Kong Stock Exchange suffered a 1% drop in share prices over a $1B trading volume when its Automatic Order Matching and Execution System reported a false 4% drop in the Hang Seng index (the main stock index at the exchange). The mistaken data caused panic selling for about 20 minutes. [RISKS 18.67]

US Senate bill 1726, the Promotion of Commerce Online in the Digital Era Act of 1996, known as the "pro-code" bill, would abolish most export restrictions and prohibit mandatory key escrow. It reached the Senate Commerce Committee on 24 Jul. The bill hearings were canceled in September.

On the underground scene, Defcon IV, a major criminal-hacker convention with participation from non-criminal elements interested in security, was held in Las Vegas, NV. One of the speakers, Netta Gilboa, publisher of *Gray Areas Magazine* and the person who harbored young fugitive Christopher Schanot, was continually harassed during her presentation and eventually had her speech ripped from her hands. This incident led to much fulmination in the DEFCON mailing list.

August

News reports in Europe announced that the US CIA has been hacking into the computers of the European Parliament and European Commission to steal economic and political secrets. Commission staff were claimed to have found evidence that the Americans had used information obtained by criminal hacking for advantages in the General Agreement on Tariffs and Trade. [*Sunday Times* 4 Aug 96, as cited in RISKS 18.30]

Scotland Yard's PBX was hacked by phone phreaks who placed about $1.5M of fraudulent calls by using direct inward services access. [Reuters 5 Aug]

The Church of Scientology settled one of its many copyright-infringement lawsuits when NETCOM On-Line Communication Services agreed to post a warning on its screens warning users not to violate intellectual property rights. The CoS often pursues redress when its religious teachings, which it describes as copyrighted trade secrets, are published without permission. [AP 5 Aug]

A correspondent on the Best of Security list reported on 9 August:

> Exploder is an ActiveX control which demonstrates security problems with Microsoft's Internet Explorer. Exploder performs a clean shutdown of Win95 and will turn off the power on machines that have a power conservation BIOS (green machines).

A few weeks later, Princeton University's Professor Ed Felten and his team discovered a security flaw in Internet Explorer 3.0 whereby an attacker could "run any DOS command on the machine of an Explorer user who visits the attacker's page. For example, the attacker could read, modify, or delete the victim's files, or insert a virus or backdoor entrance into the victim's machine." The scientists created a Web page to demonstrate the problem by deleting a file on the machine of any Explorer user who visits the page. [RISKS 18.36] In December, *Computerworld* reported, "Objects built with ActiveX can access system resources on users' desktops, which can lead to security breaches or corruption of PC data." [RISKS 18.69]

Reports about scientific studies of Internet addiction surfaced at the American Psychological Association meeting in Toronto. Dr Kimberly Young of the University of Pittsburgh gave details of the addictive behavior; e.g., spending an average of 38.5 hours a week on the Internet for personal reasons. Some addicts would use the Net in the middle of the night to avoid criticism from their families; some would claim to be ill to be able to stay home and use the Net. Sometimes abusers would extend their lunch times to three hours to be able to play on the Internet. [AP, UPI 10 Aug] Case Western University law professor Peter D. Junger filed suit in Cleveland federal court to forbid federal officials from restricting his or anyone else's ability to discuss nonclassified encryption technology with anyone worldwide or to publish that information freely. The case arose because of the professor's irritation over his perception that the ITAR prevents him from discussing encryption algorithms in his computer law class, which includes foreign students. [COMTEX News wire 12 Aug]

An emotionally-disturbed individual using the pseudonym "johnny xchaotic" claimed the blame for a massive mail-bombing run based on fraudulently subscribing dozens of victims to hundreds of mailing lists. In a rambling and incoherent letter posted on the Net, (s)he made rude remarks about famous and not so famous people whose capacity to receive meaningful e-mail was obliterated by up to thousands of unwanted messages a day. [Dow Jones 16 Aug] Someone claiming to be the same "UNAMAILER" (as the news media labeled him or her) launched a similar mass-subscription mail bombing run in late December.

In mid-August, the US Department of Justice discovered that its Web site had been vandalized. Electronic graffiti included swastikas, pictures of Hitler, images of nude women, and sophomoric satire directed at the Clinton administration and the Communications Decency Act. In addition, information about the government's programs to help abused women was defaced. [AP 17 Aug] By September, the list of vandalized Web sites included the British Conservative Party, the Nation of Islam, the American Psychoanalytic Association, and the CIA, whose site was renamed the Central Stupidity Agency on 19 Sep by Swedish cybervandals.

In Amherst, NY, thieves stole computers and storage media with information worth an estimated $250M in what appears to be outright industrial espionage directed at Interactive Television Technologies, Inc. The stolen information concerned a top-secret project to make any TV set a gateway to the Internet.

The "HDEuthanasia" virus created by the "Demon Emperor" caused a mild panic due to media exaggeration and misrepresentation in August. This so-called "Hare" virus actually was nothing special. [PA News 20 Aug, Reuters 22 Aug]

According to *Defense News* magazine, the US Army in Bosnia experienced many computer virus infections by Monkey, AntiEXE and Prank Macro viruses. Army personnel had "to waste hundreds of hours finding the viruses and cleaning them from the systems. . . ." [RISKS 18.39]

In Helsinki, Johan Helsingius protested accusations that a majority of the world's child pornography is sent via anon.penet.fi, his anonymous remailer. A short time later, he shut down the service in disgust at the trouble he was receiving from police investigations. [Reuters 28 Aug; see http://www.stack.nl/~galactus/remailers/index-penet.html]

News from the underground: The "Scriptors of Doom" criminal hacker gang begin releasing weekly exploits of security vulnerabilities in the HP-UX operating system. A criminal hacker named "Galf" began retaliating for the attacks at Defcon on Netta Gilboa by crashing the computers of those who harassed her.

September

AOL began blocking all e-mail from five Internet spammers: cyberpromo.com, honeys.com, answerme.com, netfree.com and servint.com. [AP 4 Sep] CyberPromo, one of the worst offenders against the rules of Netiquette forbidding junk e-mail, launched a lawsuit accusing AOL of infringing its right to free speech. The argument was quashed by the court in a ruling on 4 Nov. [EPIC Alert 3.19] In a related development, Concentric Network Corporation filed a lawsuit filed against Cyber Promotions and its owner Sanford Wallace on 2 Oct seeking an injunction, compensatory and punitive damages for sending thousands of junk e-mail messages fraudulently represented as coming from Concentric e-mail accounts. The spam resulted in network overload as tens of thousands of undeliverable messages were routed back into Concentric Network's mail system. Wallace and Cyber Promotions signed sworn affidavits saying they wouldn't do this any more. [See http://www.concentric.net] In November, Cyber Promotions lost another legal battle when a Philadelphia court ruled that, contrary to Cyber Promotions' arguments, AOL does in fact have a right to block spam from the prolific producer of unwanted e-mail. The judge dismissed first-amendment arguments outright, saying that there is no mandated right for anyone to force unwanted e-mail onto subscribers of an ISP. [AP 4 Nov]

In early September, an unknown criminal hacker attacked the PANIX Internet Service Provider in New York City using the "SYN-flooding attack" in which a stream of fraudulent TCP/IP requests for connections to non-existent Internet addresses overwhelms a server, denying service to legitimate users. [AP 13 Sep; RISKS 18.45] Within a week, TCP/IP specialists reported patches to prevent this denial of service attack. [For a comprehensive analysis, see ftp://info.cert.org/pub/cert_advisories/CA-96.21.tcp_syn_flooding]

Also in New York, Governor Pataki signed a new law making it a felony to transmit by computer indecent material to individuals under seventeen. The bill created a new class E felony, disseminating Indecent Materials to a Minor in the Second Degree (Penal Law Section 235.21), punishable by up to four years in state prison. [LACC-D, 12 Sep]

An interview with Margot Kidder in *People Online* revealed that a computer virus was the last straw leading to her much-publicized nervous breakdown (she was found cowering and babbling in someone's back yard). The (unidentified) virus apparently destroyed the only copy of the book she had been working on for three years -- and she had no backup. [RISKS 18.46]

According to the deputy head of the Interior ministry anti-economic crime department, Russian hackers made almost 500 attempts to access computer networks of the Central Bank of Russia from 1994 through 1996 and stole 250 billion roubles ($4.7M) in 1995. [Itar-Tass News Agency, AP 17 Sep]

A storm of protest broke when the *Tampa Tribune* and *St. Petersburg Times* received computer disks with the names of 4,000 AIDS victims from the Pinellas County Health Department. An anonymous letter accompanying the disks stated that a county health department employee had been showing people at a bar records on named people and warning his friends to stay away from the HIV+ subjects. [AP 20 Sep] The employee was fired in Oct after admitting his crime.

Penguin Books released a fraudulent advisory in the name of an imaginary Professor, Edward Prideaux, supposedly from the College of Slavonic Studies, a non-existent institution. The e-mail hoax warned readers:

> A computer virus is being sent across the Internet. If you receive an e-mail message with the subject line "Irina", DO NOT read the message. DELETE it immediately. Some miscreant is sending people and files under the title "Irina". If you receive this mail or file, do not download it. It has a virus that rewrites your hard drive, obliterating anything on it. Please surf carefully and forward this mail to anyone you care about.

The message caused concern among some of its recipients, who flooded their anti-virus vendors with requests for help against this non-existent menace. [Graham Cluley, in *Proceedings* of the International Virus Prevention Conference '97]

Phone phreaks have begun tapping into residential and home telephone lines by clipping onto circuits running through neighborhood "beige boxes" — those cabinets found on sidewalks throughout America. Pacific Bell investigators say about 10 to 15 new incidents are reported each week in California alone and they guess that the fraud is costing them several million dollars a year. [UPI 22 Sep]

In Kentucky, a former employee of Kentucky's tax collecting agency admitted stealing $4.2 million from the state treasury by using state computers to issue tax refunds to a dummy corporation he created. [AP 23 Sep]

According to Paul Engel, a San Francisco stock broker, a disagreement with an employee of the research firm SRI International Inc. led to a mail-bombing run on 23 September in which Engel allegedly received 25,000 messages consisting of the word "Idiot" sent from SRI computers. The flood of messages allegedly prevented him from using his computer, so in December Mr Engel sued SRI for $25,000 of damages [UPI 27 Dec] Regardless of the justice of the accusation, this case supports the view that corporate policies must clearly demarcate the limits of acceptable use of corporate user IDs on the Internet.

A horrified woman received hundreds of phone-calls demanding sexual services when her name and phone number were posted on the Internet as if she were a prostitute. [PA News 25 Sep]

In late September, rogue cancelbots erased 27,000 messages from various USENET groups, targeting in particular news groups used by Jews, Muslims, feminists and gays. Some of the cancelbots had racist and homophobic names. At present, it is not clear that such vandalism contravenes any laws; and attacks like this will continue unless messages on the Net become cancellable only by their uniquely identified authors. [San Jose Mercury News 25 Sep]

Kevin Mitnick was indicted in Los Angeles on 25 counts of stealing software, damaging computers at University of Southern California, using passwords without authorization, and using stolen cellular phone codes. He pleaded "not guilty." [AP, Reuters 27, 30 Sep]

In a chilling reminder of the "Good Times Virus" hoax that started in 1994, someone demonstrated how to write HTML code that hung Netscape sessions and even occasionally crashed Windows95. The Web page merely had to refer to LPT1 or COM ports as a data source. Users of Netscape as an e-mail client made the problem worse, because a user could download a "toxic" e-mail message and automatically interpret the HTML code, hanging the browser and making it impossible to delete the toxic e-mail. [http://www.pcmag.com/news/trends/t961002a.htm]

Dan Boneh, Richard A. DeMillo, and Richard J. Lipton, Bellcore cryptanalysts, showed that disrupting the normal functioning of smart cards can provide sufficient information about the encryption algorithms and keys to permit successful cryptanalysis. [EDUPAGE 1 Oct; RISKS 18.50; http://www.bellcore.com/SMART/secwp.html] Following up on this work and previous research, Israeli scientists Eli Biham (Computer Science Dept., The Technion) and Adi Shamir (Applied Math Dept., The Weizmann Institute) published a draft article, "The Next Stage of Differential Fault Analysis: How to break completely unknown cryptosystems." The abstract of the article [RISKS 18.56] read,

> The idea of using computational faults to break cryptosystems was first applied by Boneh Demillo and Lipton to public key cryptosystems, and then extended by Biham and Shamir to most types of secret key cryptosystems. [See RISKS-18.54.] In this new research announcement, we introduce a modified fault model that makes it possible to find the secret key stored in a tamperproof cryptographic device even when nothing is known about the structure and operation of the cryptosystem. A prime example of such a scenario is the Skipjack cryptosystem, which was developed by the NSA, has unknown design, and is embedded as a tamper-proof chip inside the commercially available Fortezza PC cards. We have not tested this attack on Skipjack, but we believe that it is a realistic threat against some smart-card applications that were not specifically designed to counter it.

In November, British cryptographer Ross Anderson published a draft article entitled "A serious weakness of DES." [RISKS 18.58, 18.62; www.cl.cam.ac.uk/users/rja14/tamper.html] His abstract follows:

> Eli Biham and Adi Shamir [RISKS-18.56] recently pointed out that if an attacker can induce unidirectional faults in key memory of cryptographic devices, then keys could be extracted quickly. Although their attack is very elegant, it is not practical against many fielded systems. For example, inducing a single-bit change in a DES key will cause a proper implementation to return a key parity error.
>
> However, when combined with Peter Gutman's recent work on memory remanence, there are two very practical attacks. One of them allows smartcard electronic wallet keys to be extracted with much less expensive equipment than that currently used by pay-TV pirates; the other yields an effective attack against fielded banking security modules. These attacks show that a feature of DES that had long been thought innocuous is actually a serious design error.

On the underground scene, *Phrack 48* was released under new editors; "ReDragon," "Voyager," and "Daemon9." This new issue, along with *2600 The Hacker Quarterly*, released the dangerous SYN-flooding denial-of-service source code mentioned earlier. Greg Perry, known as "Digital Hitler" in the computer underground, was arrested on charges of cellular-phone fraud.

In the September IS/Recon report, the team issued the following stern warning:

> **Plea from the I/S Recon Team**
>
> Against our efforts to secure information systems from attack the opposition continues to use open source security information to select and attack vulnerable systems. At the risk of crying wolf or being redundant, we emphasize the requirement to apply patches quickly and to work with vendors to ensure systems are up to date. The most recent, and alarming example of this is a new page at one of our "regular" hacker sites we monitor. At http://. . . is a web page that will allow you to enter host information and probe it for the httpd hole from CERT Advisory 96.06 There are logs on that site that reflect the amount of use this site and this page gets. NOTE! This includes your IP if you visit this URL. Please do not visit this URL from any of your corporate accounts. You'll be revealing your knowledge of the site, you may make yourself a target for these humans and you may contribute to our losing site of that hacker group if they shut down or realize they're under observation. Please wipe your feet on another ISP account or use CompuServe, AOL or another network to look on this site.

October

The Clinton administration announced that it would appeal the June decision against the Communications Decency Act to the Supreme Court. [1 Oct]

The administration also announced its relaxation of the ITAR. The new plan would allow companies to export programs with 56-bit keys if key recovery (key escrow, but not necessarily by government agencies) is included within two years.

The Business Software Alliance (BSA) threatened legal action against Egyptian firms, where 80% of all software is estimated to be stolen.

The BBC revealed in a news program that cellular paging services are wide open to interception and manipulation using a radio scanner and appropriate PC software. [2 Oct]

The Central News Agency of Taiwan reported that a new "political" virus was being launched to oppose Japanese claims over islands the Taiwanese call the Diaoyus. The virus would post, "The Diaoyus are the territory of the Republic of China" followed by "Don't even think of getting (the Diaoyus), Japanese monsters" and finally, the claim that the virus was written by "A patriotic teenager from Feng Hsi Junior High School." The virus would then attempt to erase data on disk.

The *San Francisco Chronicle* reported that a new e-mail-based swindle informs victims that they have only 24 hours to clear up their "outstanding account" by calling a number in the 809 area code. The long-distance call to Tortola in the British Virgin Islands costs at least $3 -- much more if victims actually listen to endless recorded messages. Peter Neumann (moderator of RISKS) adds that the e-mail's address, "Global Communications"@demon.net" is false. [RISKS 18.50]

In August 1994, Andrew Stone, 32, a convicted credit-card fraudster on day-parole from prison, was hired by *Which?* magazine editors to demonstrate the vulnerability to fraud of automated teller machines in Britain. After testing security mechanisms with the magazine's blessing, the two criminals set up an automated shoulder-surfing operations by placing cameras in several locations so they could record both the details of bank cards and the fingers of their users as they punched in their PINs. Armed with these details from two weeks of data collection, the two then created fake bank cards using gas-station premium-point cards. Apparently the particular bank victimized was chosen because its bank cards were particularly colorful and showed account information very clearly even at a distance. Stone and an accomplice then stole the equivalent of about $216,000 using stolen account information and PINs. Police finally put Stone under surveillance on a hunch and correlated the huge number of complaints about unauthorized withdrawals with Stone's presence at cash dispensers. In early October 1996, Stone was sentenced to five and a half years in prison; his accomplice received a four and a half year sentence. [PA News 4 Oct]

The Supreme Court of the US declined to hear an appeal from Robert and Carleen Thomas of Milpitas, California, who were convicted in 1994 in a landmark case affecting the definition of community in the age of cyberspace. Community standards determine whether pornographic material crosses the line into illegality. In this case, a US postal inspector in Memphis, TN downloaded material from the California BBS and arranged to file criminal charges against the two accused. They were tried in Memphis and sentenced to 37 and 30 months, respectively, in prison for sending illegal, sexually explicit files across state lines. [Reuters, 7 Oct]

The Portuguese government ordered its cellular phone service providers to install technology that would permit immediate wire tapping of any cell-phone call. [Reuters, 9 Oct]

In Colorado Springs, a software bug resulted in failure to register multiple identical ATM withdrawals on the same day from the Ent Federal Credit Union; it seems that only the first withdrawal was charged to a customer's account. Clients alerted the credit union to this problem months ago, but were ignored. In October the credit union declared that it would subtract a total of $1.2M from the accounts of 12,000 customers affected, causing much displeasure all round. [RISKS 18.53]

Professor Klaus Brunnstein of the University of Hamburg noted in mid-October that Microsoft released another CD-ROM infected with a WORD Macro virus (WAZZU.A). Apparently staff at the trade show where the infected disk was distributed shrugged off notification of the infection, saying that the virus is harmless. Infected documents were maintained on a Microsoft Web site for five days after the infection was noted. Brunnstein comments that WAZZU randomly interchanges two words in an infected document and occasionally inserts the string "WAZZU." If this is harmless, I hate to think what harmful would be like. [RISKS 18.53]

In a strike against spammers, Concentric Network, an Internet Service Provider (ISP) in northern California, obtained an injunction against notorious junk e-mailer Sanford Wallace and his Cyber Promotions company to prevent them from continuing to use or pretend to use Concentric Network accounts as the origin or reply addresses in his junk e-mail. The plaintiffs stated that the fraudulent use of their domain name caused "tens of thousands of undeliverable messages to be routed back into Concentric Network's mail system for processing and storage, resulting in the overload of Concentric's equipment and the denial of service to its subscribers." [See http://www.concentric.net]

In Hartford, CT, the Digital Technologies Group lost all their computer files and backups in what appears to have been a classic case of sabotage by a disgruntled ex-employee in mid-October. The sabotage caused $17,000 in direct costs, the loss of months of work, and a one-week shutdown that seriously damaged the company's credibility as an ISP. The alleged perpetrator was arrested in late December and faces up to 20 years in jail if convicted of the sabotage. [AP Dec 18]

Spanish police cracked an Internet child-porn ring when they arrested two young Catalonian men in Barcelona. Police around the world were reported to be cooperating in tracking down the perpetrators of these offenses, involving children as young as three years. [Reuters 10 Oct]

In the growing confirmation of the justice of the NCSA's very own Chief Executive Officer Bob Bales' belief that the Internet can be misused to create a denial of service to employers, a Nielsen Media Research survey published in mid-October suggested that employees from IBM, Apple and AT&T together spent 13,048 person-hours visiting the Penthouse World Wide Web site in a single month. Let's see, if we estimate, say, $20/hr that makes about a quarter of a million dollars of wasted pay. At Compaq, in Houston, TX, about a dozen employees were fired for logging more than 1,000 visits *each* to sex sites while they were at work. [UPI 14 Oct]

In the kind of incidents that generate rage among many observers of the Internet, twelve children in the Netherlands were injured in a single week in October by hand grenades built from detailed instructions they found on the Internet. The kids, aged 8 to 13 years, made their home-made weapons by attaching marbles, stones, and coins to firecrackers. One girl lost an eye; another was permanently hearing-impaired; the others were burned. [AP 18 Oct]

The "Ping of Death" alert was issued by Mike Bremford of the UK. Datagrams (TCP/IP packets) must not exceed 65,535 bytes. Any process which generates larger datagrams can cause a stack overflow in the operating system of a receiving machine. This is a major problem, opening practically all operating systems up to denial-of-service attacks. Patches are being spawned by the dozen by all operating systems labs. [See http://www.sophist.demon.co.uk/ping/ for more details.]

On the 22nd of October, a massive spam spread throughout the Internet, dropping thousands of fraudulent advertisements for illegal child pornography into e-mail boxes around the world. The ads fraudulently directed attention to Stephen Barnard, a resident of New Jersey who was immediately cleared by the FBI of all involvement and appeared to have been the victim of an ugly spoof. The e-mail was further disguised by forged e-mail headers pointing to two users at America Online, but investigation cleared them too. [PA News & Reuters 22 Oct]

The annual report of the French government's anti-counterfeiting task force, CNAC, reported that the Internet is useful for industrial counterfeiters. The counterfeiters send pictures of new fashions to sweatshops around the world within a day of their appearance.

During a 20-minute lunch break at a business seminar in the Strathmore Hotel in the Arndale Centre, Luton, Bedfordshire, thieves broke into the locked seminar room and stole 11 lap-top computers worth about $75,000. That's $75,000 not counting software and data. [PA News 25 Oct]

In late October, the Florida Supreme Court's home page was redesigned by persons unknown who replaced the staid wood-grained background with pictures of nude people engaged in various sexual activities. Although the site was restored to its pristine condition within a couple of days, curious Internauts raised its hit rate to new highs. [UP, Reuters 25 Oct]

Federation of Communication Services chairman Jonathan Clark, said Fraud costs the phone industry and its customers the equivalent of about $332 million a year in losses in the UK. [PA News 29 Oct]
The annual Ernst and Young information security survey results were released at the end of October. Damage from virus infections, insider attacks and outsider attacks are apparently up, but management for support for information security remains abysmal. [See http://techweb.cmp.com/iw/602/02mtsec.htm]

According to the publication "Central & East European Secure Systems Strategies (CEESSS)" (with permission of the copyright holder):

> *Secret incidents of hackers' attacks upon Czech banks and release of Czech citizens' personal information.*

by Steven Slatem <sslatem@intellitech.cz>

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, we learned in an interview at INVEX (Brno, 22 -- 26. October) with Jiri Mrnustik, CEO of the Brno-based anti-virus and encryption software developer AEC s.r.o.// (ss961112-002) (630 words) (STS)

In the four-year battle between General Motors Opel Division and Volkswagen, a German regional court threw out a civil suit for libel and 10 million marks ($6.6 million) in damages by VW against Opel. VW had filed suit with a Frankfurt court to stop Opel to cease its allegations of criminal conspiracy to commit industrial espionage against Opel and GM. The allegations began when Jose Lopez, a successful GM and Opel inventory manager defected to VW — allegedly with three cases of confidential GM documents. [Dow Jones 30 Oct] At the end of November, Lopez resigned from the board of VW. [Reuters, 29 Nov] In mid-December, he was formally charged by German police; however, VW was cleared of involvement in the industrial espionage. [Reuters, 13 Dec]

Marion Walton, an Arkansas man, was discovered having a cybersex affair with a Canadian woman. In response, his wife Pat apparently erased his mail program. In retaliation, he apparently beat her, twice. ``Police are suggesting she file charges." [Reuters 31 Oct; RISKS 18.57]

November

The Raleigh, NC *News & Observer* reported that lawyers are eager for Y2K cases. According to Christian Plumb, Bloomberg Business News. Attorney Charles R. Merrill, of McCarter & English, Newark, NJ said, "It's just a gold mine. . . . It's like a law-school case of tort issues". RISKS correspondent <stayton@ibm.net> added, "Perhaps IT managers will take better notice of the year 2000 problem -- if lawyers start getting on their case." [RISKS 18.57]

Seven men pleaded guilty in Southwark Crown Court in London to charges of criminal conspiracy to defraud British banks by tapping the communications lines between ATMs and bank computers. The captured data were to have been used to manufacture large numbers of forged bank cards. [Reuters 4 Nov]

The largest child-porn ring in the history of Canada was broken when the RCMP arrested a 22-year-old man from the remote northern Ontario town of Kirkland Lake. Police were cooperating with the FBI and cleaning up loose ends after 16 arrests of the Internet-based "Orchid Club" members from the United States, Australia, and Finland. RCMP officers seized 20,000 computer files containing photos and video clips of illegal sexual activity involving children or images of children. [AP 4 Nov]

Telephone industry executives complained that increasing Internet use is loading voice lines beyond their expected usage levels, causing increasing disruption of the US phone system. Local exchanges are producing more frequent call failures (fewer calls going through on the first try), more busy signals and calls resulting in complete silence. [Reuters 4 Nov]

An FBI investigation resulted in charges against a former employee of Standard Duplicating Machines Corporation of Andover, MA. It seems that after three years of employment with the firm ending in 1992, the employee used his knowledge of non-existent security on the firm's voice-mail system to retrieve sales leads and other valuable data on behalf of a direct competitor, Duplo U.S.A. Corporation. The alleged break-ins were aided by the use of default "passwords" for the voice-mail boxes that consisted, as is commonplace, of the extension followed by the # sign. The would-be industrial spy faces up to five years in prison a fine of up to $250,000 if convicted. [PR News wire 5 Nov] At the end of the month, the perpetrator pleaded guilty to wire fraud.

In early November, criminal hackers attacked an anti-military site [http://www.insigniausa.com] and destroyed hundreds of copied DoD documents relating to the use of chemical and biological weapons during the Gulf War. Speculation was rife that the break-in was government funded. [Newsbytes 5 Nov]

Internet Security Systems (ISS) announced the first known commercial real-time monitoring system capable of handling SYN-flooding and other denial-of-service attacks. [This note does not constitute an NCSA endorsement. See http://www.iss.net/RealSecure/]

The Canadian Radio-Television and Telecommunication Commission (CRTC) authorized phone companies' request for a ban on overnight junk fax messages in Canada during the hours of 21:30 to 09:00 on weekdays and from 18:00 to 10:00 on weekends. [Reuter 7 Nov]

The Computer Science and Telecommunications Board (CSTB) of the National Research Council (NRC) announced availability of the final version of its cryptography policy study, "Cryptography's Role in Securing the Information Society," originally released in draft form in May. [See http://www.nap.edu/bookstore for details.]

Trevor Warwick <twarwick@madge.com> reported on experiments at his site using cellular phones. His organization's usually-stable NetWare servers crashed several times for no apparent reason over a period of three days. Finally the crew noticed that each time they found the server dead, there was an AT&T technician (working on their PBX) using his cellular phone right next to the downed machine. Experimentation showed that yes, one can reliably crash a server by using such a phone within about a foot or so of the computer. On a spare server, the team found that the cell phone caused an unrecoverable system disk corruption. Keep those cell phones out of the computer room. [RISKS 18.60]

On 7-8 Nov, AT&T's WorldNet ISP suffered an 18 hour brownout in which about 200,000 customers were deprived of full access to their e-mail system. [AP 8 Nov]

Also on 8 Nov, the New York Times Web site was hit by a SYN-flood attack that caused denial of service on one of the Web's most popular sites. [See http://www.news.com/News/Item/0,4,5215,00.html]

On some commercial Web sites, improperly-installed SoftCart programs allowed unauthorized access to customers' credit card information after they bought from on-line merchants. (*Wall Street Journal* via EDUPAGE and RISKS 18.61]

There was quite a fuss (the word "debacle" comes to mind) two years ago at Lawrence Livermore National Laboratory when 90,000 sexually explicit images were found on Department of Energy computers. Apparently the improvements in security have still not penetrated some skulls. Laser physicist Kenneth Manes allegedly gave his 16-year-old son root access to a government computer used primarily for calculations for a superlaser planned as part of the lab's nuclear weapons research program. The superuser account also contained more than 90 sexually explicit images and had been used to spam a Swedish computer. Manes' 23-year old son is accused of using his illegal account to traffic in stolen software, according to documents filed in municipal court. Manes and another scientist are charged with misdemeanors in Pleasanton Municipal Court, CA.

The mid-Atlantic EPA region, responsible for federal environmental programs in PA, DE, MD, VA, WV, and DC, suffered a shutdown of its computer networks starting 6 Nov when a virus infected 15% of its workstations and servers. [AP 10 Nov]

At around the same time, someone filled the official Web page for the Latin Summit Meeting of 21 heads of state with pornography and satire. The site was hurriedly shut down by red-faced officials. [Reuters 11 Nov]

In a graphic demonstration of the harm that undated, unauthorized, immortal and unauthenticated messages circulating on the Internet can have, the Make-a-Wish Foundation set up an 800 hot line and a Web page begging for the end of one of the many variations of the Craig Shergold urban myth. Craig Shergold is a kid who had a brain tumor but it was removed and he's now fine. Unfortunately, several thousand messages a day continue to circulate among well-meaning but naive people who think that the poor chap wants their post cards and business cards. He doesn't, and neither does the postal service where he lives. Make-a-Wish have been tarred with this bizarre brush because some nitwit embroidered the story to implicate them in the scheme — and now they receive thousands of pieces of unwanted mail for someone they have never been involved with. Lesson: do NOT forward chain letters without verifying their accuracy. [See http://www.wish.org/wish/craig.html or call 800-215-1333, x. 184 for information.]
Yet more fools launched yet more virus hoaxes. One of the latest outbreak of silliness is the "Deeyenda" "virus" which supposedly does awful things via e-mail. [Details at http://www.kumite.com/myths/myth027.htm] Another stupid rumor is the PENPAL GREETINGS "virus" which supposedly does equally awful (and impossible) things. [RISKS 18.72; also http://www.symantec.com/avcenter/vinfodb.html] General urging to all: do not ever pass on "warnings" about "viruses" until you ask competent people to verify the authenticity of such warnings. [RISKS 18.73]

As if the anticipated and much-feared catastrophic meltdown of ancient computer systems still incapable of imagining dates beyond 31 Dec 1999 were not bad enough, it seems there may be real meltdowns of computer systems around that time. It happens that the 11-year solar sunspot cycle will peak around the year 2000, according to warnings from the National Oceanic and Atmospheric Administration's Space Environment Center in Boulder, CO. Some of the possible effects: surges in power lines; disruption of global positioning system satellites; interference with satellite cell phone systems; damage to computers and other electrical systems in satellites; expansion of the Earth's atmosphere and consequent perturbation of satellite and space-junk orbits; induced currents in pipelines and other large metal arrays; changes in the Earth's magnetic field, interfering with the signals used to direct oil drilling bits deep underground. I think I'll be taking *all* my money out of the banking system, preferably in gold, just before the end of 1999. [AP 19 Nov; RISKS 18.62]

USA TODAY reported on a survey of 236 major corporations prepared for a congressional committee. The evidence suggests that more than half the major corporations in America have been victimized by computer break-ins. About 58% of the companies that responded said they had experienced a break-in in the past year; almost 18% said they suffered losses of more than $1 million. Two-thirds reported losses exceeding $50,000. Respondents claimed that more than 20% of the break-ins were industrial espionage or sabotage by competitors. Companies uniformly reported concern over the negative effects of publicity of any break-ins on public confidence in their firms. [AP 21 Nov]

New York City government employees used data diddling to erase $13 million of tax records in the largest single tax fraud case in the city's history. Police officials suggested that there might be more than 200 arrests in the case; anyone convicted of fraud and bribery will face sentences of up to 10 years in prison. [22 Nov; RISKS 18.63]

Peter Garnett, 54, and his wife, Linda, 52, deposited a forged check for the equivalent of about $16.6 million ostensibly from Britain's central bank -- along with a welfare check for the equivalent of $595. It seems a propensity for crime doesn't necessarily correlate highly with intelligence. An additional clue that all was not right was the lavish lifestyle of people with no visible means of support for cruises, fancy dinners and a Rolls-Royce. The two nitwits were sentenced to three and a half years in British prisons. [AP 22 Nov]

A World Wide Web site providing news about the opposition to Belarus' hard-line president was destroyed in the last week of November. [AP 26 Nov]

On 29 Nov, Amtrak lost access to its national reservation and ticketing software--just before the heaviest travel period of the year. Agents usually had no paper schedules or fares; this lack of backup caused major delays in helping customers. [RISKS 18.64]

In the Shetland Islands, UK, a local newspaper (the *Shetland Times*) went to court to force a competing on-line daily "newspaper" (the *Shetland News*) to stop pointing to the *Times* Web page using its original headlines as links. [RISKS 18.64]. [Comments from MK: This case is reminiscent of an older debate on the Web, when a site called "Babes on the Web" began posting hypertext links to every personal Web page prepared by any woman; some women objected that such use of the links was improper. In this Scottish case, the questions are twofold: Is a headline a copyrighted work? And is a hypertext link a potential infringement of copyright? If someone posting information on a Web page can legally prevent others from linking to elements of the Web page, the implications for the Web are severe.]

On 29 Nov, a disgruntled computer technician at Reuters in Hong Kong detonated logic bombs at five investment-bank clients of the service, causing 36 hours of downtime in networks providing market information crucial for trading. The banks switched immediately to alternative services and reported no significant effects on their work; however, Reuters was deeply embarrassed by the incident. [RISKS 18.65]

On 30 Nov in Ontario, a major Canadian bank's (the CIBC's) debit-card system failed because of a flaw in a software upgrade. About half of all transactions across eastern Canada were prevented during the several hours of unavailability. [RISKS 18.65]

Phrack 49 was released with a cancelbot script and various other exploits. "Phone Losers of America," a prank-oriented phreaker group, established a headquarters for inter-state coordination.

December

A high-ranking civilian scientist working for the Department of National Defence in Ottawa was arrested on charges of trafficking in child pornography after police found large quantities of illegal materials in his account on government computers. Surely it is now unnecessary to have to come up with any more examples to convince managers that every organization needs a thorough, clear policy on appropriate use of corporate Internet resources. [Globe and Mail, 10 Dec]

Ontario Health Minister Jim Wilson resigned on the 9th of December after the government decided to investigate the actions of his former communications assistant who revealed confidential information about a doctor to *The Globe and Mail*. [Globe and Mail, 10 Dec]

An Australian telephone operator was accused of breaking into a radio station's phone line during a contest for a U$40,000 prize and ensured that he was the "lucky" 10th caller. He was investigated by police who charged him with two other cases of similar fraud. [UPI 10 Dec]

Two men admitted guilt in a corporate espionage caper. The bumblers sent Owens Corning a misspelled, ungrammatical note asking for $1,000 in return for secrets stolen from competitor PPG Industries. Patrick Worthing, 27, a supervisor at a company supply cleaning crews and operators for prototype machines at PPG, had access to every office at the PPG research center. He allegedly stole customer lists, blueprints, secret formulas, product specifications and videotapes of new machinery. Thanks to the cooperation of the intended purchaser of the information, the FBI were able to arrest the perpetrators. Ironically and pleasingly, two years ago a similar scam was addressed to executives at PPG Industries offering secrets stolen from Owens Corning; the FBI caught those spies too. Both companies insisted that it would be crazy as well as illegal to accept such information stolen from competitors. [AP 11 Dec]

Florida issued reports estimating the cost of locating and repairing Year 2000 bugs in production systems, mostly in COBOL, will cost between $88M and $120M but that it is imperative that the bugs be fixed before the end of 1999. [UPI 12 Dec]

A San Diego dentist received over 16,000 copies of the new California state tax form as a result of a computerized mailing program gone mad. [RISKS 18.68]

Someone launched a 200-message-per-second SYN-flooding denial-of-service attack on WebCom of Santa Cruz at 00:20 Saturday morning the 14th of December, blocking access for 40 hours to the Web pages of hundreds of businesses during their peak sales period. The attack was traced to someone in British Columbia and the FBI and RCMP are searching for the culprits. This was yet another incident stemming from the irresponsible publication of a detailed SYN-flood script by *2600* and *PHRACK* magazines. [AP 17 Dec; RISKS 18.69]

Slamming is the fraudulent, unsolicited switching of long-distance services to another long-distance carrier; the practice has caused consternation among victims confronted with larger phone bills than they expected from their normal carrier. In mid-December, Connecticut's Department of Public Utility Control (DPUC) was slammed by a firm called Wiltel, which converted six of its 14 lines to its service without authorization. [RISKS 18.69]

Matthew D. Healy <matthew.healy@yale.edu> reported a major hole in NCSA (National Center for Supercomputing Applications at the University of Illinois) httpd servers: any server running the phf CGI program can be tricked into sending the /etc/passwd file to any user. Mr Healy stated that several computers at the Yale School of Medicine had been compromised this way and urged readers to check their server logs to see if anyone had downloaded their password file. [RISKS 18.69] In response to many rude and offensive e-mail messages resulting from his alert, he commented that yes, the hole was known from March 1996 on, but no, he is not a full-time security expert — he just tries to manage an academic computer. [RISKS 18.70]

On 18 December, Dan Farmer, author of SATAN (Security Administrator's Tool for Analyzing Networks), released the results of a preliminary scan of some 2200 computing systems on the Internet in November - December 1996. He selected what he described as "high profile and commerce-oriented . . . Web . . . sites" plus some randomly-chosen sites for comparison. Farmer found that ". . .using simple, non-intrusive techniques, I determined that nearly two-thirds of these interesting hosts had serious potential security vulnerabilities — a rate about twice that of the randomly selected hosts!" [See http://www.trouble.org/survey]

In a small town near Copenhagen, six Danish criminal hackers who attacked Pentagon and business computers were sentenced to minor jail terms and ordered to pay fines and perform community service. One criminal hacker was sentenced to 90 days, a second to 40 days in prison. According to their defense lawyers, the criminals had "done the hacking victims a favor by exposing the vulnerability of their computer systems." [AP 19 Dec]

On 29 December, the U.S.A.F. Web page was hacked and destroyed, leading the Pentagon to pull almost all DoD Web pages off the net. [Reuters 30 Dec; AP 31 Dec]

EDUPAGE summarized the initial reactions to the Clinton Administration's "new" encryption export regulations announced in the last days of 1996:

> ENCRYPTION EXPORT POLICY TAKES EFFECT, REMAINS CONTROVERSIAL. The Commerce Department has put into effect the new rules it devised to relax the restrictions on exportation of encryption software, but the computer industry says the rules are still too restrictive and will inhibit effective competition with foreign manufacturers with powerful offerings, and a lawyer for the non-profit Electronic Privacy Information Center describes the government's strategy as a "shell game," because there's "very little functional difference" between the new rules and the old ones, which had been rejected in part by a U.S. district judge in San Francisco. "They've just moved the pea under a different shell, but the rules are the same." (Washington Post 31 Dec 96)

At the end of the year, the following satirical variation of the "Good Times" warning began circulating through the Net:

> **The latest breaking news on the GOODTIMES virus.**
>
> It turns out that this so-called hoax virus is very dangerous after all. Goodtimes will re-write your hard drive. Not only that, it will scramble any disks that are even close to your computer. It will recalibrate your refrigerator's coolness setting so all your ice cream goes melty. It will demagnetize the strips on all your credit cards, screw up the tracking on your television and use subspace field harmonics to scratch any CDs you try to play.
>
> It will give your ex-girlfriend your new phone number. It will mix Kool-aid into your fishtank. It will drink all your beer and leave dirty socks on the coffee table when company comes over. It will put a dead kitten in the back pocket of your good suit pants and hide your car keys when you are late for work.
>
> Goodtimes will make you fall in love with a penguin. It will give you nightmares about circus midgets. It will pour sugar in your gas tank and shave off both your eyebrows while dating your girlfriend behind your back and billing the dinner and hotel room to your Discover card.
>
> It will seduce your grandmother. It does not matter if she is dead, such is the power of Goodtimes, it reaches out beyond the grave to sully those things we hold most dear.
>
> It moves your car randomly around parking lots so you can't find it. It will kick your dog. It will leave libidinous messages on your boss's voice mail in your voice! It is insidious and subtle. It is dangerous and terrifying to behold. It is also a rather interesting shade of mauve.
>
> Goodtimes will give you Dutch Elm disease. It will leave the toilet seat up. It will make a batch of Methamphetamine in your bathtub and then leave bacon cooking on the stove while it goes out to chase gradeschoolers with your new snowblower.