

Computer Crime: Year 2000 in Review

ASIS Cybercrime Summit 2001

M. E. Kabay, PhD, CISSP / Security Leader

mkabay@compuserve.com

AtomicTangerine, Inc.

Wednesday 28 Feb 2001

M. E. Kabay, PhD, CISSP

Security Leader

mkabay@atomictangerine.com

Marc Goodman

Chief Cybercriminologist

mgoodman@atomictangerine.com

AtomicTangerine, Inc.

<http://www.atomictangerine.com>

Computer Crime Update

- **The IYIR project**
- **Categories used in IYIR database**
- **Today's presentation**
 - **Computer crime cases (Mich Kabay)**
 - **Computer forensics issues (Marc Goodman)**

2



It may interest the participants that the *original* version of this extract from the full two-day INFOSEC UPDATE course had 255 slides after the instructor collected them from individual modules dealing with the topics above. See the *INFOSEC Year in Review* publications for all the cases that were considered. These files will also be available with many other articles and courses by M. E. Kabay in the new *K-Files* section on SecurityPortal (<http://www.securityportal.com>).

Kabay, M. E. (1997). The INFOSEC Year in Review 1996.
http://www.icsa.net/html/library/whitepapers/infosec/InfoSec_Year_in_Review_1996.pdf

Kabay, M. E. (1998). The INFOSEC Year in Review 1997.
http://www.icsa.net/html/library/whitepapers/infosec/InfoSec_Year_in_Review_1997.pdf

Kabay, M. E. (1999). The INFOSEC Year in Review 1998.
http://www.icsa.net/html/library/whitepapers/infosec/InfoSec_Year_in_Review_1998.pdf

Kabay, M. E. (2000). The INFOSEC Year in Review 1999.
<http://www.icsa.net/html/library/whitepapers/infosec/iyir1999.pdf>

The IYIR Project

- **1993-1994**
 - **MK taught one-semester course on Information Security**
 - **Institute for Government Informatics Professionals, Govt of Canada**
- **1995**
 - **Taught update course for graduates**
 - **Reviewed developments in previous year**
- **1997**
 - **Developed database to simplify task of managing course material**

3



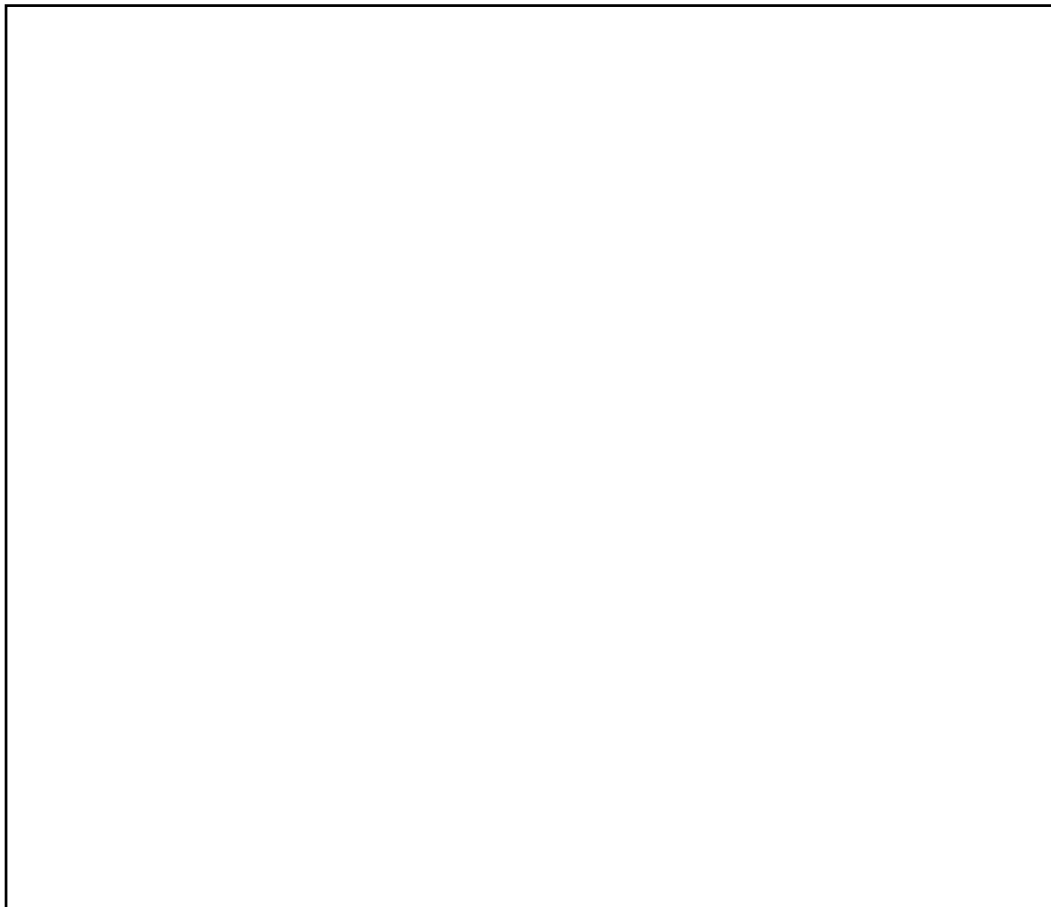
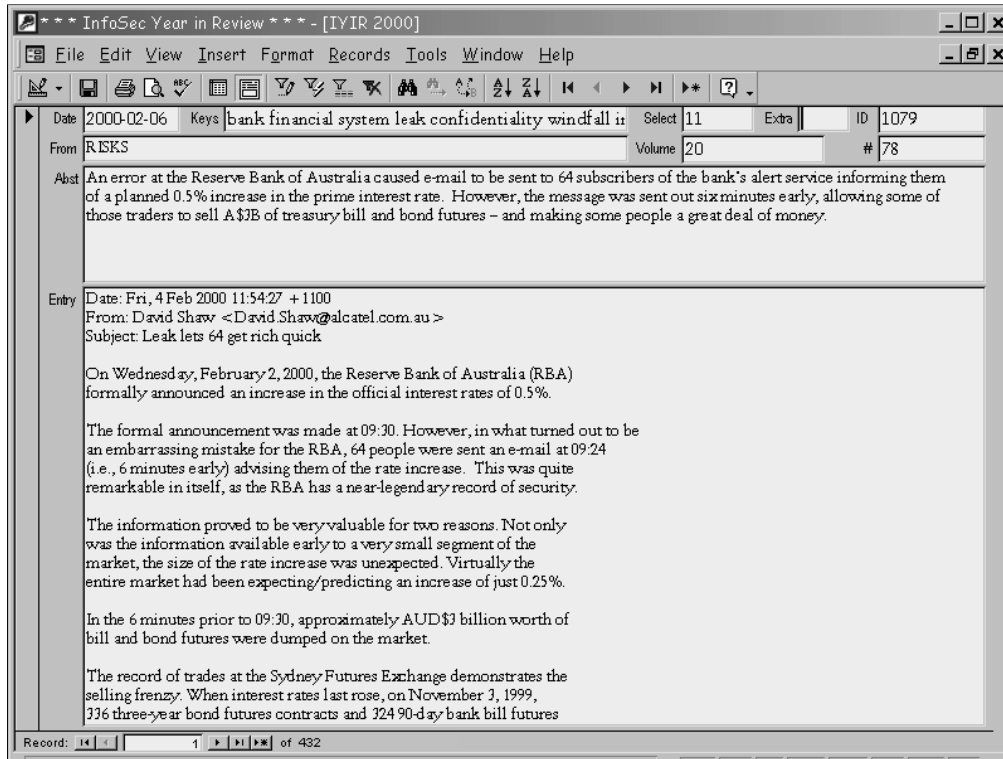
A word about copyright:

Items labeled "NewsScan" are reprinted with permission of the editors of NewsScan, John Gehl and Suzanne Douglas.

Visit < <http://www.newsscan.com> > for details of their free NewsScan newsletter and their excellent INNOVATION newsletter.

M. E. Kabay holds only the compilation copyright and the rights to his own slides and abstracts; all other quoted material remains copyright by the respective owners.

Computer Crime Review -- 2000



The IYIR Database

The screenshot displays two windows from the 'InfoSec Year in Review' application. The left window shows a tree view of categories under 'Unclassified', including 'Computer Crime (cases, indictments, convictions, sentences)', 'Breaches of confidentiality', 'Wiretapping, interception (not jamming, not eaves, law enforcement)', 'Interception', 'Data diddling, data corruption, embezzlement', 'Data corruption', 'Embezzlement', 'Viruses, worms, Trojans (assembly level or macro - not ActiveX or Java)', 'Worms', 'Trojan/spearms', 'Trojans', 'Fraud (not embezzlement, extortion, scamming)', 'Phishing', 'Exploitation', 'Spamming', 'INPOW4R, industrial espionage, botnet/ctivism', 'Industrial espionage', 'Industrial information systems sabotage', 'Infrastructure protection', and 'Military perspectives on INPOW4R'. The right window shows a detailed view of an email entry with the following text:

Date: 2000-02-06
From: RIKKS
Subject: Key bank financial system leak confidentiality windfall in
Value: 20
ID: 1079
78

An error at the Reserve Bank of Australia caused e-mail to be sent to 64 subscribers of the bank's alert service informing them of a planned 0.5% increase in the prime interest rate. However, the message was sent out six minutes early, allowing some of those trades to sell A\$10 of treasury bill and bond futures - and making some people a great deal of money.

Date: Fri, 4 Feb 2000 11:54:27 +1100
From: D'eed Shew <D'eed.Shew@telnet.com.au>
Subject: Leak lets 64 get rich quick

On Wednesday, February 2, 2000, the Reserve Bank of Australia (RBA) formally announced an increase in the official interest rates of 0.5%.

The formal announcement was made at 09:30. However, in what turned out to be an embarrassing mistake for the RBA, 64 people were sent an e-mail at 09:24 (i.e., 6 minutes early) advising them of the rate increase. This was quite remarkable in itself, as the RBA has a near-legendary record of security.

The information proved to be very valuable for two reasons. Not only was the information available early to a very small segment of the market, the size of the rate increase was unexpected. Virtually the entire market had been expecting/predicting an increase of just 0.25%.

In the 6 minutes prior to 09:30, approximately AUD\$1 billion worth of bill and bond futures were dumped on the market.

The record of trades at the Sydney Futures Exchange demonstrates the selling frenzy. When interest rates last rose, on November 2, 1999, 336 three-year bond futures contracts and 324 90-day bank bill futures

5

IYIR Source Material

- **10,000 newswire articles & newsletters/year**
- **Permission to quote abstracts directly**
 - **Edupage**
 - **NewsScan**
 - **SecurityPortal**
 - **SecurityWire**
- **Also abstracts by MK as required**



IYIR Summaries

- **Publish yearly summaries**
 - **PDF files**
 - **Date**
 - **Source**
 - **Keywords**
 - **Category**
 - **Abstract**
 - **Freely available**
- **See <http://www.securityportal.com/kfiles/iyir>**

7



Categories in the IYIR Database

- **Started with 4 areas:**
 - **Computer crimes**
 - **Emerging vulnerabilities and defenses**
 - **Management and policy issues**
 - **Cryptography, law and e-commerce**
 - **Subdivided into major areas**
- **2000**
 - **New sub-categories added**



Current IYIR Categories

- 10 Computer Crimes (cases, indictments, convictions, sentences)**
- 11 Breaches of confidentiality**
- 12 Wiretapping, interception (not jamming; not govt/law enforcement)**
 - 12.1 Wiretapping**
 - 12.2 Interception**
- 13 Data diddling, data corruption, embezzlement**
 - 13.1 Data diddling**
 - 13.2 Data corruption**
 - 13.3 Embezzlement**



Current IYIR Categories

- 14 Viruses, hoaxes, Trojans (assembly level or macro: not ActiveX or Java)**
- 14.1 Viruses**
- 14.2 Worms**
- 14.3 Virus/worms**
- 14.4 Trojans**
- 15 Fraud (not embezzlement), extortion, slamming**
- 15.1 Fraud**
- 15.2 Extortion**
- 15.3 Slamming**
- 16 INFOWAR, industrial espionage, hacktivism**
- 16.1 Industrial espionage**
- 16.2 Industrial information systems sabotage**
- 16.3 Infrastructure protection**
- 16.4 Military perspectives on INFOWAR**
- 16.5 Hacktivism**

10



Current IYIR Categories

- 17 Penetration, phreaking (entering systems, stealing telephone service)**
- 17.1 Penetration**
- 17.2 Web vandalism**
- 17.3 Phreaking**
- 18 Theft of equipment (laptops, ATMs, computers, cables, network components)**
- 19 Counterfeits, forgery (including commercial software/music piracy)**
- 19.1 Software piracy**
- 19.2 Music**
- 19.3 Movies**
- 19.4 Games**
- 19.5 Credit-cards, other tokens**
- 19.6 Legal or business documents**
- 19.7 Plagiarism**
- 19.8 Products (hardware, clothing etc.)**

11



Current IYIR Categories

- 1A Criminal hacker scene (conventions, meetings, testimony, biographies, publications)**
- 1A1 Conventions and meetings**
- 1A2 Testimony in court or committees**
- 1A3 Biographical notes on individual criminals**
- 1A4 Publications**
- 1A5 Organizations**



Current IYIR Categories

- 1B Pornography, Net-harm, cyberstalking, gambling, online auctions**
- 1B1 Adult pornography**
- 1B2 Child pornography**
- 1B3 Pedophilia, kidnapping**
- 1B4 Stalking**
- 1B5 Gambling**
- 1B6 Auctions**
- 1B7 Hate groups, speech**

13



Current IYIR Categories

- 1C Theft of identity, impersonation**
- 1C1 Impersonation**
- 1C2 Identity theft**
- 1E Law Enforcement & Forensics
(technology, organizations, proposals,
litigation, rulings, judgements)**
- 1E1 Organizations, cooperation**
- 1E2 Technology**
- 1E3 Litigation, legal rulings, judgements**
- 1E4 Government funding**

14



Current IYIR Categories

- 20 Emerging Vulnerabilities & Defenses**
- 21 Quality assurance failures (general)**
- 22 Quality assurance (security products)**
- 23 Availability issues (not denial of service)**
- 24 Mobile malicious code (JAVA, JavaScript, ActiveX; not assembly level or macro viruses)**
 - 24.1 Java**
 - 24.2 Javascript**
 - 24.3 ActiveX**
 - 24.4 HTML**
 - 24.5 Web-site infrastructure, general Web security issues**

15



Current IYIR Categories

25 RFI, jamming (not interception), HERF, EMP/T

25.1 RFI

25.2 Jamming

25.3 HERF, EMP/T

**25.4 Health effects of electronic equipment
(phones, screens, etc.)**



Current IYIR Categories

- 26 Operating systems, network operating systems, TCP/IP problems (alerts)**
- 26.1 Windows 9x/Me**
- 26.2 Windows NT/2K**
- 26.3 UNIX flavors**
- 26.4 TCP/IP**
- 26.5 LAN OS**
- 26.6 WAP (Wireless Applications Protocol)**
- 26.7 SWDR (Software-defined radio)**
- 26.8 MAC OS**

17



Current IYIR Categories

- 27 Tools for evaluating vulnerabilities**
- 28 Denial of service**
- 28.1 DoS attacks**
- 28.2 DDoS attacks**
- 28.3 DoS countermeasures**
- 29 Peer-to-peer networking**
- 2A Firewalls & other perimeter defenses**
- 2B Intrusion detection systems**
- 2C Addiction, cyber-syndromes, sociology**
- 2D Port scanning**
- 2E Online voting**

18



Current IYIR Categories

- 31 Surveys, estimates**
 - 31.1 Surveys, studies, research**
 - 31.2 Estimates, guesses, predictions, forecasts**
- 32 Censorship, indecency laws, 1st amendment (law)**
 - 32.1 USA**
 - 32.2 Non-USA**



Current IYIR Categories

- 33 Acceptable-use policies, spam & anti-spam (laws, technology)**
 - 33.1 Acceptable use**
 - 33.2 Spam**
 - 33.3 Antispam**
- 34 Net filters, monitoring (technologies)**
 - 34.1 Net filters**
 - 34.2 Usage monitoring, audit trails**



Current IYIR Categories

- 35 DNS conflicts, trademark violations (Net, Web)**
- 35.1 Cybersquatting**
- 35.2 Trademarks vs DNS**
- 35.3 Politics of the DNS**
- 36 Responses to intrusion**
- 37 Education in security & ethics**



Current IYIR Categories

40Cryptography, Law & E-commerce

41New cryptanalysis techniques

42Crypto algorithm weakness, brute-force attacks

42.1 Weaknesses

42.2 Brute-force attacks

43New I&A products (tokens, biometrics, passwords)

43.1 Tokens

43.2 Biometrics

43.3 Passwords

44New encryption algorithms, products

44.1 Algorithms

44.2 Products



Current IYIR Categories

- 45 E-commerce security, digital signature, products, digital cash, e-payments**
- 45.1 Digital signatures**
- 45.2 Digital cash**
- 45.3 Micropayments**
- 45.4 E-payments**
- 45.5 Watermarks**
- 45.6 Other e-commerce security measures**
- 46 Cryptography exports from US**
- 47 Key escrow / recovery laws**
- 48 Foreign crypto & computer crime laws (not cases or sentences)**

23



Current IYIR Categories

- 49 Privacy, consumer profiling, surveillance by law enforcement / govt, legislation, agreements**
- 49.1 International agreements**
- 49.2 EC legislation & regulation**
- 49.3 US legislation & regulation**
- 49.4 Other legislation & regulation**
- 49.5 Law enforcement**
- 49.6 Consumer profiling**
- 49.7 Trade in personal information**
- 49.8 Anonymity**
- 49.9 Industry efforts**

24



Current IYIR Categories

- 4A Evolution of Net law: framing, pointing, linking, jurisdiction**
- 4A1 Framing**
- 4A2 Pointing, linking**
- 4A3 Jurisdiction**
- 4A4 Blocking**
- 4B Intellectual property: patents, copyrights (law)**
- 4B1 Copyright**
- 4B2 Patents**
- 4B3 Reverse engineering**

25



Current IYIR Categories

- 4C Security paradigms, risk management, site-security certification, professional certification**
- 4C1 Paradigms**
- 4C2 Risk management**
- 4C3 Certification of site security**
- 4C4 Professional certification**
- 4D Funny / miscellaneous**

26



Current IYIR Categories

WHEW!

27



Breaches of confidentiality

2000-03: 485,000 credit-card #s traced to Eastern Europe

- **Stolen 1999-01**
- **Stored on US govt Web site**
- **Discovered 1999-03**
- **Issuers refused to notify victims**
- **No reports of fraud**



Breaches of confidentiality

2000-03: Raphael Gray / Wales

- **“The Saint of E-Commerce”**
- **Arrested for Internet fraud**
- **26,000 credit-card accounts**
- **US, Canada, Thailand, Japan, UK**
- **Including Bill Gates’ #**
- **E-mailed #s to NBCi**
- **“Just wanted to prove how insecure. . . .”**



Confidentiality

2000-07: MS-Hotmail leaks

- **Sending subscribers' e-mail addresses to online advertisers**
- **"Data spill"**
- **Read e-mail banner, URL goes to advertiser**
- **Hotmail puts readers' e-mail address in page URL**
- **Big firms claim to discard info**

30



NewsScan:

HOTMAIL FLAW SENDS USERS' E-MAIL ADDRESSES TO AD FIRMS

Microsoft has acknowledged that a flaw in its Hotmail program is inadvertently sending subscribers' e-mail addresses to online advertisers. The problem, which is described as a "data spill," occurs when people who subscribe to HTML newsletters open messages that contain banner ads. "The source of the problem is that Hotmail includes your e-mail address in the [Web address], and if you read an e-mail that has banner ads," the Web address will be sent to the third-party company delivering the banner, says Richard Smith, a security expert who alerted Microsoft to the problem in mid-June. Data spills are common on the Web, says Debra Pierce of the Electronic Frontier Foundation. "This isn't just local to Hotmail; we've seen hundreds of instances of data spills over the course of this year." Smith estimates that more than a million addresses may have been transferred to ad firms, but most of the big agencies, including Engage and DoubleClick, are discarding the information. (Los Angeles Times 13 Jul 2000)

<http://www.latimes.com/business/20000713/t000065732.html>

Data Diddling

Software allowed unauthorized \$\$ transfers

- **2000-01: X.com Bank**
- **Fixed**



NewsScan:

As financial institutions continue to develop online innovations, . . . electronic banking got some bad news when it was discovered that the software used by the online X.Com Bank allowed customers to transfer funds from the account of any person at any U.S. bank. All they had to know was the person's account number and bank routing information. According to the company, the dollar amounts involved in fraudulent transfer were "not significant," and the security flaw has now been corrected. But security expert Elias Levy says, "Anyone with half a clue could perform these unauthorized transfers for over a month via their Web site and create some real financial problems for other people." The company's Web site boasts that its use of technology "makes accessing and moving your money easy." (New York Times 28 Jan 2000)

ZDNet < <http://205.181.112.101/zdnn/stories/bursts/0,7407,2429909,00.html> >

Logic Bomb

2000-02: Deutsche Morgan Grenfell Inc.

- Tony Xiaotong Yu, 36, Stamford, CT
- Indicted 2000-02-10
 - NY State Supreme Court, Manhattan
- Charge: Unauthorized modifications to computer system & grand larceny
- 1996: hired as a programmer
 - End of 1996, became securities trader
- Accused of inserting programmatic time bomb into a risk model
 - Trigger date July 2000
- Months repairing the program



February 10, 2000

Man Indicted in Computer Case

By THE ASSOCIATED PRESS

A former investment bank employee was indicted yesterday on charges of programming a glitch into the bank's computer system in an attempt to cause it to lose millions of dollars.

Tony Xiaotong Yu, 36, of Stamford, Conn., pleaded not guilty at his arraignment in State Supreme Court in Manhattan on charges of computer tampering and grand larceny. Acting Justice Brenda Soloff let him remain free until today to raise bail of \$50,000.

Mr. Yu was hired by Deutsche Morgan Grenfell Inc., a division of Deutsche Bank, in February 1996 as a computer specialist to help create a program for bond traders.

In late 1996, Mr. Yu changed jobs within the bank and became a securities trader. He supposedly ended his involvement in computer programming.

But Manhattan District Attorney Robert Morgenthau said Mr. Yu secretly wrote a "time bomb" into the program he helped create, which was called a risk model. The bomb was supposed to "explode" in July, Mr. Morgenthau said.

The destructive code was found in February 1998 by other specialists who were working on the risk model program, Mr. Morgenthau said. He said programmers worked for months to undo problems created by Mr. Yu, who was dismissed after the code was found.

Mr. Morgenthau said Mr. Yu's involvement was confirmed by taped phone conversations with acquaintances.

Data Corruption

2000-01: US Natl Archives

- **Lost 43,000 e-mail messages**
- **Contractor did not make backups**
- **Admin turned off logging**
- **Assistant Archivist: "Safest backup is to print messages."**



Someone responsible for the US National Archives' e-mail system did not understand the concept of a backup. In 1999, it seems that a system problem deleted about 43,000 messages. The contractor responsible for making backups had not, in fact, been doing any. Finally, someone turned off system logging because it slowed down the system. The Assistant Archivist had a brilliant, if pessimistic, view of backups, saying, "the safest way to save important messages is to print them out".

RISKS 20.76:

Date: Tue, 18 Jan 2000 15:32:11 -0500 (EST)

From: Jeremy Epstein <jepstein@monumental.com >

Subject: U.S. National Archives loses 43K e-mail messages

The Washington Post, 6 Jan 2000, reported that the National Archives lost an estimated 43,000 e-mail messages (the number is a guess based on the number of users). The backup system also failed: the contractor was not doing as instructed (according to the Archives). The audit log, which might have shed light, had been turned off because it reduced performance.

The Assistant Archivist says that they've improved the backup system now, but "the safest way to save important messages is to print them out". Hurrah for the paperless office!

RISKS: What good are backups & audits if they're not used correctly?

Full article at

<http://www.washingtonpost.com/wp-srv/WPlate/2000-01/06/1241-010600-idx.html>

Viruses

- **2000-01: Win2K.Inta**
 - **1st Windows 2000-specific virus**
 - **Not major threat**
- **Occurrence of traditional (non-macro) viruses decreased to minor proportions**
 - **ICSA Labs *Annual Virus Prevalence Survey***
 - **Few boot-sector viruses important**
 - **File-infectors less prevalent**
 - **Macro-viruses the largest threat**
 - **Trojans also a problem**



< <http://www.f-secure.com/news/2000/20000112.html> >

First Windows 2000 Virus Found

Espoo, Finland, January 12, 2000

Virus writers already up to speed with the upcoming operating system

F-Secure Corporation, a leading provider of centrally-managed, widely distributed security solutions, today announced the discovery of the first Windows 2000 virus. Windows 2000 is the upcoming new operating system from Microsoft, due to be released later this year.

The new virus is called Win2K.Inta or Win2000.Install. It appears to be written by the 29A virus group. It operates only under Windows 2000 and is not designed to operate at all under older versions of Windows.


F-Secure has received no reports that this virus is in the wild, and it is not considered a big threat. The most important feature of the virus is its capability to spread under the new operating system. "Now we can expect virus writers to include Windows 2000 compatibility as a standard feature in new viruses", comments Mikko Hypponen, Manager of Anti-Virus Research at F-Secure.


Win2K.Inta works by infecting program files and spreads from one computer to another when these files are exchanged. The infected files do not grow in size. The virus infects files with the following extensions: EXE, COM, DLL, ACM, AX, CNV, CPL, DRV, MPD, OCX, PCI, SCR, SYS, TSP, TLB, VWP, WPC and MSI. This list includes several classes of programs that were not susceptible to virus infection before. For example, this virus will analyse Microsoft Windows Installer files (MSI files), scan them for embedded programs and infect them.

The virus contains this text string, which is never displayed:

[Win2000.Installer] by Benny/29A & Darkman/29A

Further technical information and a screenshot of the virus is available at: <http://www.F-Secure.com/virus-info/v-pics/>

<h2>Worm</h2> <p>2000-01: Haiku</p> <ul style="list-style-type: none">● F-Secure (formerly Data Fellows)● E-mail enabled virus/worm● Carrier: detailed e-mail message about Haiku generator<ul style="list-style-type: none">– actually works — Haiku in Windows box● Worm code spreads through victim's e-mail address list● Occasionally downloads and plays a .wav file from a Web site	<p>14.2</p> 
--	--

35 

< <http://www.f-secure.com/v-descs/haiku.htm> >

F-Secure Virus Information Pages

NAME: Haiku

ALIAS: I-Worm.Haiku, W95.Haiku.16384.worm

The Haiku worm usually arrives as a HAIKU.EXE file attached to an e-mail message. The message looks like it was forwarded from the original recipient with the subject 'Fw: Compose your own haikus'. The message body advertises the attached file as a Haiku (oriental poetry style) generator which it actually is. But along with Haiku generation routine the file contains worm code.

....

When the worm is run it first installs itself as HAIKUG.EXE into root Windows directory and modifies WIN.INI to be run during all further Windows sessions. After that the worm displays a messagebox with a randomly generated Haiku:

....

After system restart the worm gets control, checks if Internet connection is available and starts to look for e-mail addresses by scanning DOC, EML, HTM, HTML, RTF and TXT files. After the suitable e-mail address is found, the worm decrypts its internal message text, connects to a remote SMTP server that allows sending anonymous e-mail and sends its body MIME-encoded with the decrypted message to a found e-mail address. Then the worm displays its copyright messagebox. . . .

From time to time the worm connects to a free web hosting provider Xoom and gets a WAV file from one of user accounts. The worm writes the downloaded file as C:\HAIKU.WAV, plays it and deletes it afterwards. The WAV file has a copyright string of Sandman. . . .

Worm

2000-05: I LOVE YOU

- E-mail attachment
- Uses all addresses in address book
- May have been 27-yr-old Filipino computer student
- Became #1 infectious code in Europe, Asia, USA
- Variants appeared quickly



NewsScan:

[The I LOVE YOU computer worm struck computers all over the world, starting in Asia, then Europe. The malicious software spread as an e-mail attachment, sending itself to all the recipients in standard e-mail address books.] Within days, there . . . [were] new variations of the destructive software program popularly known as the Love Bug because it's sent as an attachment with the words "I love you" in the subject line. In one variation, the subject line purports that the message you're receiving contains a joke, and in another you're told that the message is a confirmation notice for a Mother's Day gift order. To avoid being affected by the bug, do NOT open attachments to suspicious e-mail messages. (ZDNet 5 May 2000)

[On 11 May,] Filipino computer science student Onel de Guzman of AMA Computer College in Manila . . . told authorities that he may accidentally have launched the destructive "Love Bug" virus out of "youthful exuberance." However, he would not admit that he had himself created it, saying in Tagalog: "It is one of the questions we would rather leave for the future." The name GRAMMERSoft, a computer group to which the 23-year-old man belongs, appears in the computer code of the virus, and reporters have learned that de Guzman's thesis project was rejected by AMA officials because it described a way of illegally obtaining passwords from other computer users. But investigators have not charged either de Guzman or his friend Michael Buen of any crime, nor identified them as suspects. Asked what he felt about the massive amount of damage caused around the world by the virus, de Guzman's reply was: "Nothing." (AP/San Jose Mercury News 11 May 2000)

Worm

2000-06: Timofonica

- E-mail enabled malware
- Automatically sends pager message to block of Telefonica cell phones
- Tries to delete all data on hard disk



NewsScan:

The first-ever computer . . . [worm] targeting cell phones is causing anxiety in Spain, where about 100 infections have been reported so far. The "I-Worm.Timofonica" virus works in much the same way as the ILOVEYOU . . . [worm] that wreaked havoc on computer systems last month -- it arrives as an e-mail attachment that, when opened, sends a copy of itself to everyone in the victim's Microsoft Outlook address book. For each one of those messages, it generates a random cell phone number from a block of numbers known to be used by Spanish telecom carrier Telefonica. A short message is then sent to each mobile phone, castigating Telefonica for alleged monopolistic tendencies and questionable corporate practices. As a final insult, it also attempts to delete all files on the victim's hard drive and performs several other operations that makes restoration difficult. "Two or three viruses down the road we might see these things taking out phones," warns one security specialist. (MSNBC 6 Jun 2000)

< <http://www.msnbc.com/news/417066.asp> >

Worm

2000-06: Stages

- Masquerades as ".txt" file
- Original version had lame joke about life stages
- Actually SHS file with executable code
- Masks type using Windows feature to suppress suffix



NewsScan:

A NEW VIRUS TO AVOID

A new computer virus, called "Stages," is going around and clogging the e-mail systems of some organizations. Like the recent "Love Bug" virus it multiplies by sending a copy of itself to everyone listed in the infected computer's address book; however, unlike that other virus, it masquerades as a ".txt" file even though it's really a ".shs" file that can contain executable and malicious code. Beware of opening the attachment of any e-mail message containing the words "funny," "life stages," or "jokes" in the subject line. (AP/San Jose Mercury News 19 Jun 2000)

<http://www.sjmercury.com/svtech/news/breaking/merc/docs/009074.htm>

JAPAN HIT BY COMPUTER VIRUS

There been more than 200 reported cases in Japan of a computer virus called "Stages" that invades address books in the Microsoft Outlook software of computer users who open an e-mail attachment labeled Life-Stages.txt.shs. The virus apparently originated in the U.S. If you receive an e-mail attachment of that kind, do not open it. (AP/San Jose Mercury News 3 Aug 2000)

<http://www.sjmercury.com/svtech/news/breaking/merc/docs/021805.htm>

Worm

2000-11: SONIC

- **Remote-control worm**
- **E-mail with subject "I'm your poison"**
- **Attachment GIRLS.EXE or LOVERS.EXE**
- **Trojan dropper installs process in system**
 - **Searches for payload instructions**
 - **Hard-coded reference to GeoCities site**
- **Original payload:**
 - **Back door (like BackOrifice)**
 - **Other payloads could be even worse**



The SONIC worm was found in the wild on Oct 30. This nasty remote-control worm arrived by e-mail with subject "I'm your poison" and an attachment (either GIRLS.EXE or LOVERS.EXE). If the Trojan dropper is run, it installs a core process that then searches for payload instructions on a site in the GeoCities Web-hosting service. The current payload opens a backdoor to the infected system and also monitors activity, much like BackOrifice. There were already several variants in circulation by the time the worm was discovered by Kaspersky Labs. There was some hope that the original hard-coded GeoCities site could be shut down, but it was likely that other payload-supply sites would be encoded in new variants.

See NASA Incident Response Center < http://www-nasirc.nasa.gov/nasa/whats_new.html > for more information.

Trojans

2000-08: Palm OS targeted

- **Supposedly pirated software**
- **Emulate Nintendo Gameboy on Palm PDA**
- **Deletes applications on PDA**



NewsScan:

VIRUS TAKES AIM AT PALM PDAs

Software companies have reported that the first virus to target the Palm operating system has been discovered. The bug, which uses a "Trojan horse" strategy to infect its victims, comes disguised as pirated software purported to emulate a Nintendo Gameboy on Palm PDAs and then proceeds to delete applications on the device. The virus does not pose a significant threat to most users, says Gene Hodges, president of Network Associates' McAfee division, but signals a new era in technological vulnerability: "This is the beginning of yet another phase in the war against hackers and virus writers. In fact, the real significance of this latest Trojan discovery is the proof of concept that it represents." (Agence France Presse/New York Times 29 Aug 2000)

<http://partners.nytimes.com/library/tech/00/08/biztech/articles/30palm-virus.html>

Trojan

2000-10: QAZ invades Microsoft networks

- **Passwords sent to e-mail address in St Petersburg, Russia**
- **Resided on systems 12 days**
- **New accounts created**
 - **MS claimed no theft/damage of source code**
 - **Intruders may have examined source code**
- **Progress: major company dealt with problem openly**
 - **Forthright public statements**
 - **Worked with FBI to gather evidence**

41



NewsScan:

Microsoft's internal computer network was invaded by the QAZ "trojan horse" software that caused company passwords to be sent to an e-mail address in St. Petersburg, Russia. Calling the act "a deplorable act of industrial espionage," Microsoft would not say whether or not the hackers may have gotten hold of any Microsoft source code. (AP/New York Times 27 Oct 2000)

However, within a few days, Microsoft . . . [said] that network vandals were able to invade the company's internal network for only 12 days (rather than 5 weeks, as it had originally reported), and that no major corporate secrets were stolen. Microsoft executive Rick Miller said: "We started seeing these new accounts being created, but that could be an anomaly of the system. After a day, we realized it was someone hacking into the system." At that point Microsoft began monitoring the illegal break-in, and reported it to the FBI. Miller said that, because of the immense size of the source code files, it was unlikely that the invaders would have been able to copy them. (AP/Washington Post 30 Oct 2000)

* * *

Symantec Anti-virus Research Center (SARC) News:

Trojans in the News

Moderate[3] PC

=====

W32.HLLW.Qaz.A was first discovered in China in July of 2000. As of Aug 9 2000, SARC has received over 70 submissions and believes this threat to be in the wild. Qaz.Trojan is a backdoor Trojan that will allow a remote hacker to connect and control the machine. It is network aware and is able to spread over a local area network in a worm like fashion. When launched it will search for a copy of notepad.exe and rename it to note.com. It will then copy itself to the computer as notepad.exe. Each time notepad.exe is executed, it will run the Trojan and notepad to avoid being noticed. It will also modify the following system registry key to execute itself every time the system is booted.

....

Fraud

2000-01: SEC vs. Tokyo Joe

- **Web-based stock advice**
- **Sold own shares in stocks he urged readers to buy**



NewsScan:

SEC ACCUSES TOKYO JOE

The Securities and Exchange Commission has filed a civil lawsuit against Yun Aoo Oh Park (known as "Tokyo Joe" on the Web site where he dispenses stock market advice), charging him with defrauding investors by selling his own shares in stocks that he was urging his readers to buy. First Amendment lawyer Floyd Abrams says: "The position of the S.E.C. is not ridiculous and cannot be blown away by hoisting a First Amendment banner, but the case does raise a serious First Amendment issue involving the continued availability of the Web as a place where people can speak broadly in an uninhibited manner about topics, including the stock market." (New York Times 6 Jan 2000)

* * *

Fraud

2000-09: Emulex pumped and dumped

- **Bogus press release from 23-yr-old Mark Jakob**
- **Claimed bad profits, CEO resignation**
- **Dow Jones & Bloomberg ran stories based on fiction**
- **60% drop in share prices in 15 minutes**
- **Jakob made \$240,000 in profits**
- **Father said he was proud of his son for being so smart**



NewsScan:

FBI ARRESTS EMULEX HOAX SUSPECT IN CALIFORNIA

A former employee of online press release distributor Internet Wire was arrested Thursday and charged with securities and wire fraud in connection with the distribution of a phony press release that sent a tech company's stock price plummeting last week. Shares of Emulex, a maker of fiber-optic equipment, lost up to 60% of their value, most of it during one 15-minute freefall, after some financial news services, including Dow Jones and Bloomberg, ran stories based on the release. The bogus release claimed the company had issued a profits warning, that it was being investigated by securities regulators, and that its CEO had stepped down. The stock eventually recovered most of its value after the company denied the reports. The suspect, 23-year-old Mark Jakob, allegedly used a computer at El Camino Community College to construct and send the release, and then initiated a series of trades that netted him profits of \$240,000. (AP/Investors Business Daily 1 Sep 2000)

<http://www.investors.com/editorial/tech05.asp>

Fraud

2000-09: SEC conducts 4th Internet Sweep

- 33 companies, individuals
- Pump & dump scams
- Total fraud >\$10M
- Accused include bus mechanic, college student, car-service driver



NewsScan:

SEC SWEEP NETS 33 FRAUDSTERS

Days after arresting the California man responsible for the Emulex hoax, U.S. Securities and Exchange Commission officials conducted its fourth major "Internet sweep," taking action against 33 companies and individuals accused of using the Internet to defraud investors in classic "pump and dump" stock scams. Enforcers cited manipulation of more than 70 microcap or penny stocks, which are more loosely regulated than Big Board shares and have long been the target of illegal trading activities. "Thinly traded microcap stocks are particularly susceptible to online manipulations," says Richard H. Walker, SEC director of enforcement. "That's why we have made this area one of our highest enforcement priorities." The individuals and companies charged on Wednesday had allegedly reaped illegal profits totalling more than \$10 million. Many of the individuals had no experience in stock trading, and included a bus mechanic, a college student and a car-service driver. (Financial Times 7 Sep 2000)

<http://www.ft.com/>

Fraud

2000-10: More Internet (dot-com) executives shady?

- **Kroll Associates study of 70 .com execs**
- **4x more likely to have "unsavory background" than other executives**
- **Results of due-diligence investigations**
 - **27 had problems (39%)**
 - **Normally expect only 10%**
- **Problems:**
 - **SEC violations, insurance fraud**
 - **Links to organized crime, FCPA violations**



NewsScan:

Internet executives are four times more likely to have "unsavory backgrounds" than execs from other industries, according to a study by corporate security firm Kroll Associates. Over the past six months, Kroll has carried out 70 due diligence background checks of dot-com executives and board members, and about 39% -- 27 people -- were found to have problems -- much higher than the typical 10% that Kroll expected. Problems included: violations of Securities and Exchange Commission rules, insurance fraud, undisclosed bankruptcies, frauds committed overseas, and even links to organized crime. In one of the most extreme cases, two people that Kroll was investigating because they had made an unsolicited offer to invest in a U.S. dot-com company were later murdered. "In the course of the law enforcement investigation they found the two were connected to penny stocks promotional scams and organized crime," says Ernie Brod, executive managing director of Kroll's New York office. Most of the problems were not associated with the inexperienced management teams who frequently run dot-coms, but rather with "gray beards" brought in to add stature to the company. "I refer to these people as vampire investors," said Brod. "Maybe they put a couple of bucks in, then they lick their lips at the opportunity and suck exorbitant consulting fees out of them, or put their relatives on the payroll." (Financial Times 24 Oct 2000)

Extortion

CD Universe penetrated, threatened, harmed 1999-12

- **19-year-old Russian criminal hacker "Maxus"**
 - broke into Web site, stole credit-card data
 - 300,000 customers affected
- **\$100,000 to fix bugs, "forget your shop forever"**
 - else sell cards & announce to news media
- **Company refused extortion**
 - posted 25,000 accounts on Maxus Credit Card Pipeline Web site 1999-12-25
- **Lightrealm hosting service took site down 2000-01-09**



Credit Card Crook

APf 1/10/00 2:14 PM

NEW YORK (AP) -- A computer hacker who claimed to have stolen 300,000 customer credit card numbers from an Internet music store posted thousands of the numbers on a Web site after his attempt to extort money from the company failed, The New York Times reported today.

The company, CD Universe, refused to pay the hacker's demand of \$100,000. The unknown extortionist claimed in e-mails to the Times that he used some of the credit card numbers to obtain money for himself.

The hacker, believed to be based in Eastern Europe, for two weeks used a Web site to distribute up to 25,000 of the stolen numbers, said Elias Levy of SecurityFocus.com, a computer security firm. The site was shut down Sunday morning.

CD Universe and its parent, eUniverse, were working with the FBI to track the hacker.

"He definitely has CD Universe data," said eUniverse chairman Brad Greenspan. "Whether he hacked the site or got the data in some other way, I'm not sure exactly."

The company was notifying customers of the theft and was working with the credit card companies to help holders of stolen card numbers.

The hacker, identifying himself as Maxim in an e-mail to the Times, said he exploited a security flaw in the software used to protect financial information at CD Universe's Web site. He said he sent a fax to the company last month offering to destroy his credit card files in exchange for \$100,000. When he was rebuffed, he said, he began posting the numbers on another Web site, called Maxus Credit Card Pipeline, on Christmas Day.

The hacker e-mailed the Times the numbers for 198 credit cards as proof of the theft. The numbers were real, said the Times, which contacted the credit card owners. At least one owner confirmed she had been a CD Universe customer.

Extortion

- **2000-01: VISA International hacked**
 - Extortionist demanded \$10m for return stolen information
 - Visa said info worthless — no threat visa or customers
 - Extortion investigated by police
 - No arrests
- **2000-01: ICC admits banks caved to extortionists**
 - Long-running questions about bank extortion
 - Intl Chamber of Commerce confirmed cases



WSJ(1/19): Visa: Hacker Stole Computer Data, Demanded Ransom

From *The Wall Street Journal*

LONDON (AP) -- Visa International said that a computer hacker demanded a \$10 million ransom for information stolen from the credit-card company's electronic databank.

Visa said the information stolen last July from its European headquarters here consisted of old, low-level files and posed no threat to customers or its ability to process transactions.

"They didn't get anything to do with customer information or PIN numbers or anything that could reasonably constitute a security threat to us or our customers," spokesman Chris McLaughlin said.

Mr. McLaughlin said that Visa's computer experts moved quickly to shore up its electronic defenses in July after learning of the security breach and that the hacker didn't return.

The company received a ransom demand in early December but refused to pay anything, instead notifying Scotland Yard and the U.S. Federal Bureau of Investigation of the blackmail attempt.

Scotland Yard confirmed that it is investigating the case, under Britain's Computer Misuse Act of 1990. No arrests have been made.

The incident came to light just a week after a computer hacker stole credit-card numbers from an Internet music retailer in the U.S. and released thousands of them on a Web site when the company refused to pay a \$100,000 ransom.

The New York Times received an e-mail from a self-described 19-year-old from Russia who claimed to have taken 300,000 card numbers from customers of the music retailer, CD Universe. The parent company of CD Universe, eUniverse Inc. of Wallingford, Conn., didn't know how the Web site was violated or how many customers may have been affected.

Copyright 2000 Dow Jones & Co., Inc. All rights reserved.

Extortion

2000-02: Cartes Bancaires case

- Serge Humpich analyzed smart-card authentication
- Asked for equiv. of \$1.5M
- After demo, arrested, fired
- 10-month suspended sentence
- Controversy: attacks claim case discourages helpful analysis



< http://www.infowar.com/hacker/00/hack_012700a_j.shtml >

1/27/00 Smart Card Crypto Genius Sent to Trial

A French computer programmer has landed himself in the soup, after designing a spoof credit card that could (The Guardian reports) "talk any cash terminal into handing him an unlimited supply of money".

Serge Humpich, 36, was arrested when he offered his invention for £20 million to French banks. Humpich was in court on Friday, Jan 21, where the "procureur général" (i.e. state prosecutor, the French equivalent of a US district attorney) demanded a two-year suspended jail sentence along with FFfr50,000 (roughly £5,000) in fines. Sentencing is due on February 25.

Humpich's invention exploited flaws in the design of French electronic point of sale systems and could pick out all 35 million French PINs used on Visa and other credit cards. His discovery could also call into question the security of the smart card micro-chips used, until recently, in all French credit cards. New smart cards introduced by The GCB (Groupement des Cartes Bancaires) are supposed to be fool-proof. However the GCB's claim that smart cards are now 'bug free' amount to little more than hot air if the fault lies with the terminals.

"I didn't discover a crack in the system," Humpich said appearing in a Paris court (The Guardian reports). "I showed the card company managers that the entire system from A-Z was unsafe. The group which controls the use of credit cards did not believe me so I showed them I could fool any terminal by cracking the basic mathematical formula based on 96 numbers."

Humpich is charged with using spoof credit cards to buy 10 Paris Metro tickets from an automatic dispenser. He made this transaction and then sent the receipt to the credit card company, to prove that his spoof card worked without being detected.

The spoof credit card could not, as the The Guardian reported, "talk any cash terminal into handing him an unlimited supply of money": it worked only with terminals that did not send online referrals to the credit card network. So the card could be used only to buy cheap items (less than £10)-- hence the reason why Humpich bought Metro tickets to demonstrate his claims.

Humpich was arrested in September 1999, three months after making contact with the credit card control group. He says he had no intention to steal, pointing out he could have posted his "crack" on the Internet, enabling other programmers to make their own credit cards from micro-chip-fitted blank cards. Also, by offering to provide the banks with a defence against the crack,

Humpich was doing the honourable thing, his lawyer argues. . . .

Extortion

- **2000-12: Creditcards.com threatened**
 - **55,000 credit-card numbers stolen**
 - **Thief threatened to publish #s on Net**
 - **Demanded ransom of \$100,000**
- **Company refused, contacted FBI**
- **Criminal published the #s + rant**
 - **Claimed he wanted contract to improve security**



NewsScan:

The FBI . . . [began] searching for a network vandal who stole 55,000 credit card numbers from a private portion of the Creditcards.com Web site and published them on the Internet after the company refused to pay the intruder money in order to keep the information from being circulated. . . ." (New York Times 13 Dec 2000)

Slamming

2000-06: WorldCom slammed

- **FCC investigation showed slamming**
- **\$3.5M settlement**
- **President B. J. Ebbers said incidents perpetrated by a few employees only**



WORLDCOM PAYS \$3.5 MILLION TO SETTLE "SLAMMING COMPLAINT"

Long-distance company WorldCom Inc. is paying \$3.5 million to settle an inquiry by the Federal Communications Commission into 2,900 complaints from persons charging that WorldCom telemarketers switched them away from other phone service carriers using a deceptive practice known as "slamming." WorldCom president Bernard J. Ebbers says the slamming incidents "were perpetrated by a few sales employees who have since been terminated." (Washington Post 7 Jun 2000)

<http://www.washingtonpost.com/wp-dyn/articles/A10351-2000Jun6.html>

Industrial Espionage

1999-11: Legal firm accused of espionage

- 1st lawsuit involving industrial espionage by lawyers
- Moore Publishing (Wilmington DE) sued Steptoe & Johnson (Washington DC)
 - allegedly breaking into computer systems $\geq 750X$
 - stolen user-ID & password
- Systematic cyberwar
 - misinformation posted on newsgroups
 - HotMail account traced to defendants
- Damages at least \$10M



Computer Hacking Suit Escalates Against Top U.S. Law Firm

WASHINGTON, Nov. 11 /PRNewswire/ -- Moore Publishing Co. Inc., has expanded its computer hacking case against Washington D.C.-based law firm Steptoe & Johnson, LLP.

The lawsuit represents the first time a top U.S. law firm is accused of hacking into another company's computer systems. The case is also believed to represent one of the first documented cases of corporate versus corporate computer hacking in the U.S.

Moore Publishing, an investigative information research firm based in Wilmington Delaware, filed an amended complaint in U.S. District Court for the District of Columbia this week, alleging that Steptoe & Johnson conspired to repeatedly hack into certain internet domains as well as the computer systems hosting the targeted internet sites owned by the company.

The case seeks more than \$10 million in damages.

According to the suit, Steptoe & Johnson hacked into the domains and the system servers more than 750 times, while at the same time used a stolen password and e-mail identity of a Virginia businesswoman during the attacks, apparently to cloak the law firm's electronic attacks. "The alleged misconduct in this case involves serious violations of state and federal criminal laws, with ramifications far beyond this civil suit," said Rodney R. Sweetland III, attorney for Moore Publishing.

The suit also alleges Steptoe & Johnson repeatedly used the Virginia woman's stolen e-mail identity to launch a "cyber war" against Moore Publishing and its president, by posting numerous defamatory messages throughout an internet newsgroup. The defamatory e-mail postings, including usage of an anonymous Hotmail account, however, were eventually traced to the prestigious law firm, according to papers filed in the suit. . . .

Industrial Espionage

1999-11: Alibris, Interloc sued over intercepted e-mail

- Alibris company paid \$250K fine on behalf of acquisition
- Interloc admitted intercepting & copying 4,000 e-mail messages sent to Amazon.com
 - Went through own ISP Valinet
- To gain competitive advantage against Amazon?
- Interloc's business managers denied any wrongful intention
 - failed to explain why they copied e-mail



<http://www.sjmercury.com/cgi-bin/edtools/printpage/printpage.pl>

Online bookseller charged in intercepting e-mails

Posted at 3:12 p.m. PST Monday, November 22, 1999 BOSTON (Reuters) -

Alibris, an online rare bookseller pleaded guilty to intercepting e-mails between its clients and online retail giant Amazon.com, the U.S. Attorney's office in Boston said Monday.

Alibris agreed to pay \$250,000 to settle criminal claims by U.S.

Attorney Donald Stern that it intercepted e-mail messages to its clients from Amazon.com. Alibris, of Emeryville, Calif., said it no longer offers clients email service, but its corporate predecessor, Interloc Inc, did.

Stern's office contends that Interloc intercepted the messages between its customers and Amazon.com in part to gain commercial advantage by gathering information on its customers' purchases and obtaining market data.

Alibris admits to the wrongdoing but said it gained no commercial advantage because it already knew what its customers were buying.

Rather, according to President and Chief Executive Martin Manley, the company broke the law when it tried to rectify complaints from some clients who said they weren't receiving e-mail messages from Amazon.com. In tracking such messages to determine the problem, the company unlawfully captured the messages, although Manley said it did not read them.

``The conclusions reached by the government in this, with respect to motive, are not necessarily ones we share," Manley told Reuters.

Assistant U.S. Attorney Jeanne Kempthorne, who is prosecuting the case, said there is no evidence anyone suffered financial harm as a result of the conduct, which occurred in 1998 and involved nearly 4,000 electronic messages.

But, she added, ``I think the violation of privacy is a material harm."

Industrial Espionage

2000-06: Microsoft trashed

- **Several non-profit watchdogs used Dumpster diving on MS**
- **Oracle Chairman L. J. Ellison defended trashing as civic duty**



NewsScan:

TRASHING MICROSOFT

Microsoft is complaining that various organizations allied to it have been victimized by industrial espionage agents who attempted to steal documents from trash bins. The organizations include the Association for Competitive Technology in Washington, D.C., the Independent Institute in Oakland, California, and Citizens for a Sound Economy, another Wash., D.C.-based entity. Microsoft says, "We have sort of always known that our competitors have been actively engaged in trying to define us, and sort of attack us. But these revelations are particularly concerning and really show the lengths to which they're willing to go to attack Microsoft." (Washington Post 20 Jun 2000)

<http://www.washingtonpost.com/wp-dyn/articles/A22819-2000Jun19.html>

* * *

ORACLE DEFENDS TRASHING OF MICROSOFT

Saying he was exercising a "civic duty," Oracle chairman and founder Lawrence J. Ellison defended his company of suggestions that Oracle's behavior was "Nixonian" when it hired private detectives to scrutinize organizations that supported Microsoft's side in the antitrust suit brought against it by the government. The investigators went through trash from those organizations in attempts to find information that would show that the organizations were controlled by Microsoft. Ellison, who, like his nemesis Bill Gates at Microsoft, is a billionaire, said, "All we did was to try to take information that was hidden and bring it into the light," and added: "We will ship our garbage to [Microsoft], and they can go through it. We believe in full disclosure." "The only thing more disturbing than Oracle's behavior is their ongoing attempt to justify these actions," Microsoft said in a statement. "Mr. Ellison now appears to acknowledge that he was personally aware of and personally authorized the broad overall strategy of a covert operation against a variety of trade associations." (New York Times 29 Jun 2000)

<http://partners.nytimes.com/library/tech/00/06/biztech/articles/29tech.html>

Industrial Espionage

2000-07: EC worried about Echelon

- **US-initiated global surveillance**
- **Extensive automated analysis of voice calls**
- **European Parliament formed temporary committee**
- **Investigate suspected industrial espionage**



NewsScan:

EUROPEAN PARLIAMENT EYES SPY SYSTEM

The European Parliament has renewed its attack on the U.S.-devised Echelon satellite and eavesdropping network by forming a "temporary committee" to investigate whether the spy network was used for commercial espionage against European businesses. The parliament said the committee will also determine Echelon's legality. Echelon, which is jointly operated by the U.S., the U.K., Australia, Canada and New Zealand, is capable of intercepting phone, fax and e-mail signals around the world and is intended to gather intelligence regarding terrorist and other threats to the U.S. and its allies. (Newsbytes 6 Jul 2000)

<http://www.newsbytes.com/pubNews/00/151697.html>

IS Sabotage

1998: Java implementation corrupted

- Sun Microsystems accused Microsoft of violating license
- Internal documents referred to “corrupting” Java
- Goal: prevent Java from becoming effective cross-platform environment
 - Could compete with Windows
- 2000-01: judge reinstated injunction barring MS from distributing MS-Java



January 26, 2000

Microsoft Is Told to Abide by Sun on Java

By THE ASSOCIATED PRESS

SEATTLE, Jan. 25 -- A federal judge has ruled that Microsoft must conform to standards set by Sun Microsystems when it sells products that use Sun's Java programming language.

The judge, Ronald Whyte of the United States District Court, amended a preliminary injunction that said Microsoft would be in violation of Sun's copyright on the Java language as well as in violation of its contract with Sun if it shipped products that failed to conform to Sun's standards.

An appeals court had overturned the earlier order because of the copyright element. Judge Whyte dropped that part of the ruling in his amended order.

The ruling came in a lawsuit that Sun filed in October 1997, accusing Microsoft of trying to extend the Java language for special use with its Windows operating system, which Sun contends is a violation of both the contract and the Java copyright.

Michael Morris, general counsel for Sun, said the company was happy with the decision by the judge

Jim Cullinan of Microsoft said the amended ruling showed that Microsoft did not harm competition through its actions but merely that a contract dispute existed over the companies' licensing agreement.

Microsoft is still barred from shipping its versions of Java, and other issues in the suit remain unresolved.

Java, introduced by Sun in 1995, allows developers to write a software application that can run on a variety of computers, regardless of the underlying system. Sun has tried to promote Java as a universal programming language.

Critical Infrastructure Protection

1999-11: Information Technology Association of America (ITAA) Statement of Principles

- Importance protecting national information infrastructure
- Private industry: primary authority
- Lowest possible government regulation in critical infrastructure protection
- Call for distinctions among cyber-mischief, cybercrime, cyberwar
- Appropriate law enforcement agencies take charge specific cases
 - minimal jurisdictional confusion
 - assurance clear legal basis for prosecution



<http://www.ita.org/infossec>

STATEMENT OF PRINCIPLES

In developing industry positions on national InfoSec issues, ITAA has established a list of general principles that should guide the development of future policy.

- * The protection of the national information infrastructure must be based on the minimum amount of government (federal, state, and local) regulation as is feasible.
- * The cost of protecting the national information infrastructure must be kept to the lowest level possible commensurate with the threat and the consequences of attack. Parties must be able to differentiate between potential vulnerabilities and specific threats.
- * Industry owns and operates the Global Information Infrastructure and, as such, should have primary authority for InfoSec requirements, design and implementation.
- * Industry and government share an interest in the proliferation of a free and open Internet, electronic commerce, other value-added networks, and an efficient, effective information infrastructure generally.
- * In protecting these resources, the specific and immediate priorities of government and industry are apt to diverge.
- * Industry will be guided by business considerations to protect itself against physical and cyber-attack as the threat to the information infrastructure evolves.
- * Industry encourages and supports efforts by the Federal government to coordinate its own InfoSec programs and activities to avoid duplicative efforts within the Federal government.
- * Where corrective InfoSec action is required to protect the public good, government must identify such instances and create appropriate research, development and funding mechanisms to ensure correct reaction.

(Cont'd on next page)

Computer Crime Review -- 2000

(Cont'd from previous page)

- * The Internet and electronic commerce are inherently global in nature; therefore, information security will require collaboration among international bodies.
- * InfoSec measures must be commensurate with the threat involved; risks must be appropriately identified and managed but not magnified or embellished.
- * Positive interaction between government and industry is essential. Among issues that will require on-going communication and assessment is the need to balance the Constitutional right to privacy with national security concerns.
- * Industry must monitor the private sector portion of the national information infrastructure and should cooperate both internally and with government in reporting and exchanging non-proprietary information concerning threats, attacks, and protective measures. Coordination among principals must facilitate creation of early warning systems.
- * In creating the information infrastructure, as well as attendant tools and technologies, industry must be provided safe harbor protections and its works viewed as incidental to losses caused by criminal or malicious misbehavior or natural disasters.
- * Distinctions must be made among cyber-mischief; cyber-crime and cyber-war to clarify jurisdictional issues and determine appropriate responses. The adequacy of current laws to prevent these threats must be reviewed.
- * Existing laws must be adapted as necessary to allow appropriate levels of information sharing among companies, and between the private sector and government.
- * Current policy in areas such as the R&E tax credit, software encryption, workforce training and long-term government research, and development funding must be reviewed in light of common InfoSec goals and objectives.
- * Law enforcement agencies must gain sufficient cyber-crime expertise to combat specific threats and to investigate specific criminal acts.
- * Emergency response organizations must gain sufficient disaster recovery expertise to minimize the effect of catastrophic events on the information infrastructure.

Implementing this diverse set of principles will require substantial work, resources, and cooperation.

The Information Technology Association of America (ITAA) provides global public policy, business networking, and national leadership to promote the continued rapid growth of the IT industry. ITAA consists of 26,000 direct and affiliate corporate members throughout the U.S., and a global network of 39 countries' IT associations. The Association plays the leading role in issues of IT industry concern including taxes and finance policy, intellectual property, telecommunications competition, workforce and education, encryption, critical infrastructure protection, online privacy and consumer protection, securities litigation reform, government IT procurement, and human resources policy. ITAA members range from the smallest IT start ups to industry leaders in the Internet, software, IT services, ASP, digital content, systems integration, telecommunications, and enterprise solution fields. For more information visit <<http://www.ita.org>>

Infrastructure Protection

- **2000-02: US AG Janet Reno — “wake-up call”**
 - **Must prosecute computer crimes**
 - **Disapproved of plan for Thompson-Lieberman OMB centralization of infrastructure protection**
- **2000-02: AAAS Annual Meeting**
 - **Panels concurred about INFOWAR as threat**
 - **Urged intl cooperation to catch/prosecute criminals**
- **2000-03: Presidential Directive**
 - **Fed agencies must assess vulnerability**

58



NewsScan:

RENO CALLS DDOS “WAKE-UP CALL”

In the wake of the distributed denial-of-service attacks, US federal officials debated the appropriate responses to the high-profile interference with e-commerce. Attorney General Janet Reno said publicly on 2000-02-07 that the attacks were a “wake-up call” to improve Web security and to catch criminal hackers. However, she did not endorse proposals by FBI Director Louis Freeh to prosecute criminal hackers under US anti-racketeering statutes. She did strongly support criminal prosecution, however: “We've got to help define, by our prosecutions based on real crimes, what you can and can't do on the Internet,” she said.

* * *

MK:

At the American Association for the Advancement of Science (AAAS) meeting in Washington, DC, panelists from government and from private industry concurred that information warfare is a real threat to the United States. Speakers urged better cooperation among law enforcement officials around the world to catch the culprits responsible for attacks on systems and network; they also supported changes in international law to allow extradition of suspects. Sceptics such as Kevin Poulson scoffed that if the infrastructure were as vulnerable as infowar proponents claimed, we'd have no electricity.

* * *

NewsScan:

CLINTON WANTS U.S. AGENCIES TO TIGHTEN COMPUTER SECURITY

A new presidential directive has been issued requiring U.S. government agencies to assess their vulnerability to cybervandalism. Chief of Staff John Podesta will work the agencies to put together a government-wide plan, and President Clinton says, “We must do more to uphold Americans' high expectations that their right to privacy will be protected online.” (Bloomberg/USA Today 3 Mar 2000)

<http://www.usatoday.com/life/cyber/tech/cth501.htm>

Infrastructure Protection

- **2000-08: Richard Clarke supports CIP**
 - **1st Infrastructure Coordinator, National Security Council**
 - **Encourage ISACS (Information Sharing and Analysis Centers)**
 - **Perhaps amend FOIA**
 - **Support INFOSEC research (\$600M)**
 - **Share classified info with “trusted partners”**
- **2000-12: Push for US Federal CIO**
 - **Oversee all INFOSEC for federal government**
 - **Prepare for defense against information warfare**

59



MK:

In August, Richard Clarke, the National Security Council's first Infrastructure Coordinator, called on industry to strengthen their own information security as a means of strengthening national security: "By protecting the IT security of your company, you can protect the security of your country." He listed several ways the US government is trying to improve information security:

- * Supporting Information Sharing and Analysis Centers (ISACs), which are industry-specific groups of companies sharing information about INFOSEC;
- * Possibly amending the FOIA (Freedom of Information Act) to reduce ISAC participants' fears of being forced to reveal sensitive information if they talk to government and law-enforcement officials about cybercrimes;
- * Supporting INFOSEC research by spending \$600M, especially in areas not immediately attractive to the private sector;
- * Sharing classified information with "trusted partners."

NewsScan:

Speaking at a computer security conference, National Security Council member Richard Clarke told the audience that the next president of the U.S. should appoint (and get Congressional confirmation of) a government-wide chief information officer with authority to oversee all of the government's security. "What this presidential election year showed is that statistically improbable events can occur. It may be improbable that cyberspace can be seriously disrupted, it may be improbable that a war in cyberspace can occur, but it could happen." Clarke said that certain other nations have created information-warfare units and are "creating technology to bring down computer networks." (AP/USA Today 8 Dec 2000)

Military Perspectives on INFOWAR

2000-02: Taiwan warns of INFOWAR from PRC

- **Taiwan Research Institute seminar**
- **Beijing committed to R&D in INFOWAR**
- **Asymmetric warfare: cheap attacks, costly defenses**
- **Acquire defense secrets through technological espionage**
- **Attack strategic information systems, weaponry/warfare systems in 1st strike**
- **Sabotage non-military infrastructure (telecomm, finance, electricity, traffic)**



TAIWAN RESEARCHERS WARN AGAINST "INFORMATION WARFARE" BY CHINA.

Text of report in English by Taiwanese news agency CNA

Taipei, 19th February: The Republic of China needs to guard against the possible use of "information warfare" by mainland China, researchers at a think tank warned during a seminar on Saturday [19th February].

Taiwan Research Institute (TRI) convened the one-day seminar on the topic of mainland China's information warfare research and development and its effect on Taiwan at the Taipei International Convention Centre. The seminar was presided over by Lin Bih-jaw, deputy secretary-general to President Lee [Li] Teng-hui [Deng-hui]

TRI researchers noted that Beijing has been dedicated to the research and development of its information warfare capabilities in recent years, adding that its progress in this field has greatly upgraded mainland China's combat capabilities.

The researchers said information warfare, which causes minimum personal casualties, is less costly, and can be utilized rapidly for a quick strike, is ideal to Beijing's notion of "unification (with Taiwan) first and rule (the island) later." They said that Beijing, which has been able to obtain high-tech nuclear weapons, intercontinental missiles, and artificial satellites, could also acquire information technology and therefore pose a more serious threat to Taiwan's security.

They said that Beijing, based on the principle of taking Taiwan in a single strike, could employ its advanced information technology edge to intercept Taiwan's strategic information and interfere with its weaponry and warfare systems. Beijing could also bring Taipei to its knees by sabotaging non-military systems, such as its telecommunications networks, and its financial, electrical and traffic systems. Beijing could also launch a disinformation campaign to create social disturbances and demoralize the local population in order to create a pretext for invading Taiwan, the researchers warned. . . .

Source: Central News Agency, Taipei, in English 1109 gmt 19 Feb 00.

BBC Worldwide Monitoring/ (c) BBC 2000.

Hacktivism

- **2000-01: WTO Web site attacked in Nov**
 - 700 probes
 - 54 attempted penetrations
 - “Electrohippies” tried DoS attack
- **2000-01: Japanese Web sites defaced**
 - Rape of Nanking (1937)
 - Major damage, propaganda messages
- **2000-02: South American wave of DoS**
 - Few sites adequately protected



RISKS 20.77:

Date: Wed, 26 Jan 2000 07:14:39 -0800 (PST)

From: "Ole J. Jacobsen" <ole@cisco.com>

Subject: **Japanese Government Websites hacked**

Japan called an emergency meeting Wednesday to boost computer security after humiliating raids on government Websites by hackers, who linked one to a pornographic site and attacked Japan's war record on another. The announcement came amid revelations that the site at the Science and Technology Agency had been penetrated twice in two days, and that key data on another site, including census information, had been erased.

[Source: http://dailynews.yahoo.com/h/nm/20000126/wr/japan_hackers_4.html,

Japan Calls Emergency Meeting As Hackers Hit Again, By Elaine Lies,

Reuters, 26 Jan 2000; via Dave Farber's IP list]

* * *

MK:

Throughout Latin America, cybervandals went on a rampage in the weeks following the high-profile distributed denial-of-service attacks that hit prominent Web sites in the US e-commerce community. Many of the criminal hackers posted propaganda about the Elian Gonzalez case. Security experts commented that the INFOSEC situation in South and Central America is even worse than in the US and Europe, with few sites adequately protected against intrusion and limited knowledge of computer security among law enforcement authorities there.

Hacktivism

2000-02: Balkan cyberconflicts

- **Armenian, Azerbaijani criminal hackers**
- **“Liazor” Armenian hackers altered newspaper text**



MK:

In the Balkans, the ancient hostilities among different communities continued to have cyberspace repercussions. Armenian and Azerbaijani criminal hackers vandalized Web sites run by various organizations in each others' countries. Accusations flew through the news media about misinformation campaigns and one group, the Armenian hacker collective calling itself Liazor, actually changed the text in newspaper articles. "It wasn't a punitive action, we simply wanted to oppose spreading computer vandalism," said a Liazor spokesman, Gevork. [Hmm, opposing vandalism by vandalism. . . . Is that like having intercourse for virginity? Killing for peace?]

Penetration

2000-01: AOL vandal sentenced

- **Jay Satiro, 19 — former AOL tech support volunteer**
- **Caused estimated \$50K damages**
- **Pled guilty**
- **On probation for forging money orders**
- **1 year in jail, barred from computer contact**



MK:

In New Rochelle, NY, a former volunteer for AOL technical support was sentenced to one year in jail for breaking into AOL and causing \$50K in damages. Jay Satiro, 19, was described by his own lawyer as, "a disturbed young man." After pleading guilty of computer tampering, he was barred from having a computer in his room or computer access in his home. Judge M. Perone's severity may have been influenced by Satiro's having committed the latest offence while on probation for having used forged money orders to buy computers.

USA Today < <http://www.usatoday.com/life/cyber/tech/ctg955.htm> >

Penetration

2000-01: Global Hell gang member arrested

- **16-yr-old boy from Eldorado, CA**
- **Stole 200,000 user IDs and passwords for PacBell ISP**
- **Had decrypted 63,000 passwords**
- **Boasted about theft in chat rooms**
- **May have been responsible for 26 other penetrations, incl. Harvard University computer systems break-in**



NewsScan:

HACKERS STEAL PASSWORDS, CAUSE HAVOC

A 16-year-old hacker, one of a group calling themselves Global Hell, infiltrated Pacific Bell's Internet service and lifted codes to the accounts of 200,000 subscribers. When Eldorado, Calif., detectives checked his bedroom last week, they found that he'd decrypted 63,000 of those accounts, causing PacBell to advise those subscribers to change their passwords. Authorities found the boy after he broke into the computers of an Eldorado Hills Internet service provider and began bragging about his exploits in a chat room. According to a sheriff's detective, the same teenager hacked into 26 other sites, including a master computing system at Harvard, before he was arrested Dec. 14. Authorities expect to charge him with unlawful computer access and grand theft next month. (Los Angeles Times 12 Jan 2000)

<http://www.latimes.com/business/20000112/t000003535.html>

Penetration

2000-03: "Max Vision" indicted

- 27-yr-old Max Ray Butler, Berkeley CA
- Charges of entering govt computers
 - NASA, Argonne Natl Labs, Brookhaven Natl Labs, Marshall Space Ctr, DOD
- Had been govt informer — helped FBI on computer crimes



NewsScan:

MAN INDICTED FOR VANDALIZING GOVERNMENT COMPUTERS

Twenty-seven-year-old Max Ray Butler of Berkeley, California, has been indicted on charges of breaking into and causing damage to government computers belonging to such agencies as NASA, the Argonne National Labs, the Brookhaven National Lab, the Marshall Space Center, and various facilities of the Department of Defense. Butler (also known as "Max Vision") has in the past been an FBI source, helping the Bureau solve computer crimes. (AP/San Jose Mercury News 23 Mar 2000)

<http://www.sjmercury.com/svtech/news/breaking/merc/docs/008604.htm>

* * *

See also

<<http://www.csmonitor.com/durable/2000/03/28/text/p3s1.html>>

<http://www.fedcirc.gov/news_2000.html>

Penetration

2000-09: juvenile sentenced to 6 months

- 16-yr-old from Florida
- Broke into govt computers, including NASA, Pentagon
- AG Janet Reno: "Breaking into ... property...is a serious crime."



NewsScan:

JUVENILE GOES TO JAIL FOR NETWORK VANDALISM

A sixteen-year-old Florida boy has been sentenced to six months in a federal detention center for having used the Internet to break into government computers, including ones operated by NASA and the Pentagon. Attorney General Janet Reno said, "Breaking into someone else's property, whether it's a robbery or a computer intrusion, is a serious crime." (AP/New York Times 22 Sep 2000)

<http://partners.nytimes.com/2000/09/22/technology/22AP-HACK.html>

* * *

See also

<<http://partners.nytimes.com/2000/09/22/technology/22AP-HACK.html>>

Web vandalism

- News is that there are so many cases of Web vandalism that this is *no longer news*.
- See defaced-site mirrors
 - <http://www.attrition.org/>
 - <http://www.antionline.com/archives/pages/>



Theft of equipment

2000-09: CEO of Qualcomm robbed

- **Irvin Jacobs gave speech to journalists in Irvine, CA**
- **Left his IBM ThinkPad on floor of hotel conference room**
- **Stolen**
- **Had just told audience of unencrypted proprietary info on laptop of possible interest to foreign governments**

USE DISK ENCRYPTION!

68



NewsScan:

THEFT OF QUALCOMM EXEC'S LAPTOP PC

After addressing a national business journalists' meeting in Irvine, California, Qualcomm chief executive Irvin Jacobs found that someone had stolen his laptop computer, which he left on the floor of a hotel conference room. The thief acquired not only an IBM Thinkpad but also the Qualcomm secrets it contains, because Jacobs had just finished telling the audience that the slide-show presentation he was giving with his laptop contained proprietary information that could be valuable to foreign governments. People in the area "included registrants, exhibitors and guests at our conference, hotel staff and perhaps others." Qualcomm, a leader in the wireless industry, and is the world's leading developer of a technology known as CDMA, which makes high-speed Internet access available on wireless devices. (Reuters/San Jose Mercury News 18 Sep 2000)

<http://www.sjmercury.com/svtech/news/breaking/ap/docs/4122581.htm>

Piracy: Software

2000-05: FBI arrests 17 *Pirates with Attitudes*

- Warez sites
- 5 former low-level engineering employees at Intel
- Potential U\$250K fines & 5 yrs in prison



NewsScan:

FBI NABS 17 INVOLVED IN SOFTWARE PIRACY

The FBI has arrested 17 people, five of them former or current employees of Intel, on charges of involvement with Internet sites devoted to pirated software. The five were described as having held low-level engineering jobs, and an Intel spokesman said four out of the five were no longer with the company. All 17 suspects were members of a loosely organized group called Pirates with Attitudes, which operated one of the Internet's oldest "warez" sites – a term describing a hacker variation of software sold in stores by merchants. Most warez sites are run as hobbies and their users are often teenage boys who view downloading a pirated software program to be a rite of passage. The indictments do not allege that the perpetrators were attempting to make money through their activities, but the potential penalties include a US\$250,000 fine and five years in prison. "This is the most significant investigation of copyright infringement involving the use of the Internet conducted to date by the FBI," says a spokeswoman for the Bureau's Chicago office. "It demonstrates the FBI's ability to successfully investigate very sophisticated online criminal activity." (Wall Street Journal 5 May 2000)

<http://interactive.wsj.com/articles/SB957492236169474418.htm>

Piracy: Software

2000-08: Gamara, the Flying Turtle

- **AOL's software for wireless communications**
- **Pirated copies distributed through Web**
- **10,000 downloads**



NewsScan:

COPIES OF AOL'S WIRELESS SOFTWARE FLOATING IN CYBERSPACE

America Online says that an unauthorized distribution of its new software for wireless devices poses no danger to the privacy of AOL users, though about 10,000 people have download the software from the Web in the past few days. Carnegie Mellon University computer science professor Mahadev Satyanarayanan thinks the release of the software (code-named Gamara, for the flying turtle monster that battled with Godzilla) could give clues about how to hide out on AOL's systems. Gamera uses Mozilla, a browser made by Netscape, which was purchased by AOL in 1998. (Washington Post 17 Aug 2000)

<http://www.washingtonpost.com/wp-dyn/articles/A38427-2000Aug16.html>

Piracy: Music

- All year: Napster in the news for facilitating music exchange
- 2000-09: MP3.com ordered to pay \$117M in damages to Universal Music Group
- 2000-09: Grateful Dead come out against music piracy



JUDGE CALLS MP3.COM DEFENSE 'FRIVOLOUS'

U.S. District Judge Jed Rakoff says MP3.com is using "indefensible" and "frivolous" arguments in its defense against charges of copyright violations brought by the Recording Industry Association of America. The judge, in ruling against MP3.com, determined that the company "is replaying for the subscribers converted versions of the recordings it copied, without authorization, from plaintiffs' copyrighted CDs. On its face, this makes out a presumptive case of infringement." Rakoff called MP3.com's fair-use defense "indefensible" and its claim that it was protecting record companies from music pirates "frivolous." (Bloomberg/Los Angeles Times 5 May 2000)

<http://www.latimes.com/business/20000505/t000042406.html>

* * *

JUDGE RULES MP3.COM VIOLATED MUSIC COPYRIGHTS

A federal judge has ruled that MP3.com willfully violated music copyrights and has ordered it to pay at least \$117 million in damages to Seagram's Universal Music Group -- believed to be the largest copyright infringement penalty in history. "This should send a message that there are consequences when a business recklessly disregards the copyright law," says a senior VP of the Recording Industry Association of America, which represents Universal and the four other major music companies. "We trust this will encourage those who want to build a business using other people's copyrighted works to seek permission to do so in advance." The industry's lawsuit claimed that MP3.com had violated copyright laws by creating a database of 80,000 unauthorized CDs, and the judge's ruling assessed a \$25,000 penalty for every Universal CD illegally posted on its My.MP3.com service -- somewhere between 4,700 and 10,000 recordings. MP3.com says it will appeal the ruling, which it called "draconian." (Los Angeles Times 7 Sep 2000)

<http://www.latimes.com/business/20000907/t000083988.html>

Piracy: Music

2000-10: Survey shows widespread support for music trading

- **Pew Internet & American Life Project**
- **53% general Internet users reject downloading=stealing**
- **78% active downloaders reject copyright**
- **21% of downloaders buy CD of what they download**



NewsScan:

MUSIC DOWNLOADING IS NOT THEFT, SAYS MAJORITY OF AMERICANS

Downloading music off the Internet is not stealing in the eyes of 53% of all U.S. Internet users, according to a new study by the Pew Internet & American Life Project. And those who are active downloaders are even more adamant about their position -- 78% do not believe that downloading and sharing files for free is wrong, and 61% don't care if the music they're downloading is copyrighted. Even among the general population, 40% of those surveyed said they didn't see anything wrong with downloading music off the Internet, while 35% said the downloaders are stealing, and 25% chose not to take a position. In a finding guaranteed to raise the ire of the Recording Industry Association of America, only 21% of music downloaders end up actually buying the music they get off the Internet. (E-Commercetimes 2 Oct 2000)

<http://www.ecommercetimes.com/news/articles2000/001002-1.shtml>

Piracy: Music

2000-10: MP3 negotiates agreement with NMPA

- **National Music Publisher's association**
- **3 year agreement**
- **\$30M in reimbursement for past use**
- **Advance royalty payments on future use**



NewsScan:

MP3 TO PAY \$30 MILLION TO MUSIC PUBLISHERS

Under the terms of a tentative 3-year agreement between the National Music Publishers' Association and online music company MP3.com, MP3 will pay music publishers as much as \$30 million to reimburse them for past uses of their music and to make advance royalty payments on future uses. MP3's 80,000 album collection was originally created without the permission of the publishers and recording companies that own the copyrights to the music. (Reuters/San Jose Mercury News 18 Oct 2000)

<http://www.mercurycenter.com/svtech/news/breaking/internet/docs/5277521.htm>

Piracy: Movies

- **2000-01: DVD encryption cracked**
 - Jon Johanson, 16, from Norway
 - Created and distributed DeCSS
 - Charged with copyright violation
- **2000-07: Johanson testifies in 2600 trial**
 - Eric Corley charged with copyright infringement
 - Posted DeCSS on 2600 Web site
 - Corley ordered to remove DeCSS from site



NewsScan:

CHARGES FILED FOR CRACKING DVD ENCRYPTION

A Norwegian teenager and his father have been charged in Oslo for developing a program for cracking DVD security codes and distributing it through the Internet on the father's home page. Norwegian news reports indicate that the two defendants will be the first in the world to face criminal charges involving digital versatile disks. (AP/New York Times 26 Jan 2000)

<http://www.nytimes.com/library/tech/00/01/biztech/articles/26disc.html>

* * *

MK:

The ongoing legal battle between the owners of movies on DVDs and criminal hackers who distributed the DeCSS program that allows unauthorized computer access to the copy-protected materials had a visitor from Norway in late July: Jon Johansen, the 16-year-old who wrote DeCSS with two other hackers in 1999. Mr Johansen's testimony was dismissed as irrelevant by the attorneys for the plaintiffs, but the judge wearily allowed the youngster to speak. "The man is here from Norway. I may as well hear it," he said. Mr Johansen's father Per said that his son was carrying on a proud tradition as a freedom fighter. [Helping people make illegal copies of movies is equivalent to fighting the Nazis??]

* * *

See also

< <http://www.nytimes.com/library/tech/00/07/cyber/cyberlaw/21law.html> >

Piracy: Games

2000-07: Sega cracks down

- 60 Web sites, 125 auction sites
- Sold pirated Dreamcast games
- Used Digital Millennium Copyright Act of 1998
- Web-hosts and auction sites held accountable



NewsScan:

SEGA DECLARES WAR ON PIRACY SITES

Sega has shut down more than 60 illegal Web sites and 125 auction sites selling pirated versions of its Dreamcast games, which until recently had been viewed as a "Fort Knox of online intellectual properties" -- protected by far more sophisticated technology than the relatively simple music, film and video files targeted by services like Napster and Scour. Despite the security precautions, several dozen Dreamcast titles were released this month on the Internet and have been traded via networks like Internet Relay Chat (IRC). Charles Bellfield, Sega's director of communications, says his company's actions mark one of the first times that the Digital Millennium Copyright Act of 1998 has been invoked to go after the Web-hosting companies and ISPs used by pirate traders. "It is the first time that this act has been used not just to stop piracy, but also physical sales over the Internet. It is the first time that Web-hosting companies and Web auction sites are being held accountable for the contents of what is being sold." (Reuters 20 July 2000)

<http://www.techweb.com/wire/sstory/reuters/REU20000720S002>

Forgery: Plagiarism

- Sites for professors in battle against plagiarism
- Compare student paper with banks of existing papers from plagiarism sites
 - <http://www.plagiarism.org/>
 - <http://www.canexus.com/>
 - <http://www.cs.berkeley.edu/~aiken/moss.html>
 - <http://www.integriguard.com/>



NewsScan:

BRILLIANT OR PLAGIARIZED? COLLEGES USE SITES TO EXPOSE CHEATERS

Although the Internet has made it easier for students to plagiarize assignments, a number of different Web sites now help professors identify plagiarized materials. For example, Plagiarism.org compares student papers submitted by professors to those available from free online cheating sites. In addition, the site searches papers from past semesters and from other schools to find potential plagiarism. The company sends an e-mail report to the professor, pointing out phrases that should be checked more carefully. Professors must then determine for themselves whether the material has actually been plagiarized. Another anti-plagiarism service called Essay Verification Engine can even discover instances of plagiarism where students have changed words or hidden plagiarized content in the middle of a paper. Anti-plagiarism companies say dozens of schools are trying out the services, with fees usually starting at about \$20 a year for a 30-student class. (New York Times, 20 Jan 2000)

See also

< <http://www.nytimes.com/library/tech/00/01/circuits/articles/20chea.html> >

Biographical Notes on Individual Criminals

- **2000-01: Kevin Mitnick released on parole**
- **2000-07: Mitnick wins right to write, speak, consult**
- **2000-09: Mitnick astonishes world by asserting that people are weakest link in security**
 - Spoke to IT directors at conference
 - “In God we trust. Everybody else is suspect.”
 - “Ask yourself not if, but when, is your e-business going to be targeted?”

77



NewsScan:

MITNICK LAWYERS SAY SPEAKING BAN VIOLATES FIRST AMENDMENT

Ex-convict network hacker Kevin Mitnick, out on parole but forbidden by the court to write or speak about the computer industry, is being represented by New York attorney Floyd Abrams, an expert on the First Amendment to the Constitution, which guarantees freedom of speech. Abrams has been retained by publisher Steven Brill, who wants to use Mitnick as a columnist for the Contentville Web site. (CNet/New York Times 25 May 2000)

http://www.nytimes.com/cnet/CNET_0_4_1951220_00.html

* * *

HACKER MITNICK IS BACK ONLINE

Kevin Mitnick, a hacker who had been barred, under a 1995 plea agreement, from any contact with computers, cell phones or any other device capable of connecting to the Internet, has won the right to pursue computer-related work. Following his release from prison in January, Mitnick's probation officer had also prohibited him from speaking publicly or writing about technology-related issues, and from holding any job that could give him access to a computer. Mitnick challenged the limitations, and a federal judge agreed that the restrictions were overly broad. Among the jobs now approved are: writing for Steven Brill's online magazine Contentville, speaking in Los Angeles on computer security, consulting on computer security, and consulting for a computer-related TV show. Mitnick spent five years in prison after the FBI fingered him in a series of attacks on companies, including Motorola, Novell, Sun Microsystems and the University of Southern California. (AP/CNet 13 Jul 2000)

<http://news.cnet.com/news/0-1005-200-2250843.html?tag=st.ne.ron.lthd.ni>

Grey-Hat Hackers

2000-01: L0pht members join AtStake

- Eight members of L0pht Heavy Industries
- Formed new consulting firm called AtStake
- Continue to use hacker handles (e.g., Mudge, Weld Pond, Space Roague, Brian Oblivion, Dildog)
- Described in glowing terms by some reputable experts
- Other commentators not impressed

78



1. Described in glowing terms by some reputable experts
 - Counterpane's Bruce Schneier: "They're very, very good -- first rate. . . ."
 - NTBugtraq's Russ Cooper: "The eight brilliant geniuses down at the L0pht. . . ."
2. Other commentators not impressed
 - John Taschek of PC Week: horror at the move
 - ". . . farmer giving the fox the key to the chicken coop. . . ."
 - ". . . L0pht's history shows that the group is not ethical, maintained practices that bordered on being illegal and is simply downright scary. . . ."

Adult Pornography Online

2000-07: WAPP

- **Wireless Application Protocol Porn**
- **“Key indicator of future success is whether it supports porn.”**



NewsScan:

PORN SITES SIGNAL WAP ACCEPTANCE

Analysts say the appearance of the first WAP (wireless application protocol) pornography sites signals the adoption of WAP technology into the mainstream. Although the sites offer only tiny grainy images of naked Japanese models, sociologists say that the key to predicting whether a new technology will take off is to determine whether it's used for pornography: "It's inevitable, I suppose, that with any new technology people will use it for porn," says David Birch, CEO of Consult Hyperion. "That's been the story with photography and video cameras." The news should be welcomed by wireless companies, which have reported slower growth rates than they had hoped. (The Independent 8 Jul 2000)

<http://www.independent.co.uk/news/Digital/Update/2000-07/wap080700.shtml>

Child Pornography Online

2000-01: Activists form Condemned.org

- **Dedicated to eradicating child porn online**
- **Legal means: notification of LEOs, SysAdmins**
- **Illegal means: hacking, data destruction**
 - **Can ruin evidence needed for prosecution**



MK:

In mid-December 1999, a group of activists and technology experts formed Condemned.org, dedicated to eradicating child pornography, pedophile sites and child exploitation on the Internet. The group uses legal means such as notifying law enforcement and system administrators of the presence of child porn on their servers; most immediately terminate the accounts responsible. However, the group warns, if there is no action taken, some of the members turn to illegal tactics. In such cases, members will hack into vulnerable sites and wipe entire hard drives. Some opponents of child pornography protest that these illegal methods destroy the evidence needed by law enforcement to locate and prosecute malefactors.

Child Pornography Online

2000-11: Metatags used to divert kids to porn

- **Envisional (UK) found 12,000 cases of toy names used for porn sites**
- **“My Little Pony,” “Barbie,” “Muppets”**
- **Illegal use of trademarks**
- **Difficult to enforce laws**
 - **Jurisdictional problems**



NewsScan:

[In November, an article in the Financial Times reported that pornographers were] using "metatags," the labels attached to Web pages that identify their contents, to draw visitors seeking information on the holiday season's most popular toys, with the result that children surfing the Web for My Little Pony, Barbie or Muppets could find among their choices not only toy retailers but such sites as www.picturesofanalsex.com. Envisional, a UK company that specializes in searching the Net for trademark violations, said it has found nearly 12,000 examples of toy names being used this way. A British attorney noted that using registered trademarks in this way is illegal, as is using metatags to drive children toward obscene material, but that such laws were difficult to enforce, given the worldwide reach of the Internet. (Financial Times 16 Nov 2000)

Pedophilia, Kidnapping

2000-06: testimony before US Congress

- **Estimated 3,000 kids kidnapped by abductors met on Net**
- **Survey of teenage girls: 12% agreed to meet strangers after online contact**
- **Children between 2 and 7 are fastest growing cohort of users**



NewsScan:

INTERNET KIDNAP WARNING

Child safety experts warned the U.S. congressional committee on child online protection yesterday that with the average of age of online users declining, children increasingly are put at risk by their careless or ignorant online activities. Parry Aftab, a children's advocate, told committee members that 3,000 children were kidnapped in the U.S. last year after responding to online messages posted by their abductors. A recent survey of teenage girls found 12% had agreed to meet strangers who'd contacted them online. Children between the ages of two and seven are among the fastest growing user cohorts. (Financial Times 9 Jun 2000)

<http://www.ft.com/>

Online Gambling

- **2000-02: # cybercasinos grew from 15 in 1996 to 700 in 2000**
 - Revenue ~\$1.5B in 2000, \$3B in 2002
 - US residents account for ~50% of revenue
- **2000-08: Offshore Internet Gambler sentenced**
 - Site based in Antigua for sports bets
 - US court ruled physical location irrelevant
 - Sentenced owner Jay Cohen to 21 months in federal prison



NewsScan:

ONLINE GAMBLING ON TRIAL

The future of online gambling could be decided in a trial starting this week that pits the U.S. Justice Department against the World Sports Exchange (www.wsex.com), an online betting operation based in Antigua. The importance of the case goes beyond gambling, however, says one Internet attorney: "This is an interesting case of asserting jurisdiction over overseas Web sites in a criminal context. It will be closely followed by companies doing business on the Internet, both in the U.S. and abroad." The attorney prosecuting the case maintains that where the bet is placed physically doesn't matter; the crime occurs when an "interstate wire communication facility" like the Internet is used to transmit the wager. But Internet legal experts disagree, pointing out that legislation aimed at banning Internet gambling has not yet been passed in the House of Representatives. "This pushes the concept of jurisdiction to its limits," warns Henry Judy, a member of the American Bar Association's committee on cyberspace law. (Financial Times 14 Feb 2000)
<http://www.ft.com/>

* * *

ONLINE GAMBLER GOES TO PRISON

A co-owner of an online offshore gambling business based on the Caribbean island of Antigua has been sentenced to 21 months in a U.S. prison for violating this country's federal Wire Wager Act, which makes it illegal to use telephone lines in interstate or foreign commerce to place sports bets. The prosecutor noted: "An Internet communication is no different than a telephone call for purpose of liability under the Wire Wager Act." (Reuters/New York Times 11 Aug 2000)

<http://partners.nytimes.com/library/tech/00/08/biztech/articles/11gambling.html>

Online Gambling

- **2000-10: Nevada accepts online betting**
 - **Nevada Gaming Control Board**
 - **24-hour bets on football, horse races, etc.**
 - **Federal laws prohibit transmitting bets over state lines**
- **2000-12: Maryland allows online lottery tickets**
 - **“Just the beginning in gaining access to this large and demographically desirable market niche,” -- Maryland Lottery Director**
 - **Illegal to pay for lottery using credit cards**



NewsScan:

For the first time, an online-gambling site has received approval to operate in the U.S. The Nevada Gaming Control Board has okayed Virtgame.com's plan to run an online betting parlor for football games, horse races and other sports. "Twenty-four hours is one of the beauties of the Internet," says a book manager for Coast Resorts, which owns four Las Vegas casinos, "but it could be a monster to manage." Virtgame has a contract with Coast to provide the computer system for Coast's online sports-betting sites, and is now marketing its system to others in the gambling business, including state lotteries. States have jurisdiction over all types of gambling within their state lines, but federal laws still prohibit transmitting bets over state lines. (Wall Street Journal 13 Oct 2000)

See

Wall Street Journal < <http://interactive.wsj.com> >

Online Auctions

- **2000-02: FTC declares war on online auction fraud**
 - **10,000 complaints in 1999 (107 in 1997)**
 - **No jurisdiction for fraud in overseas Web sites**
- **2000-05: France bars participation in foreign online auctions**
 - **Pay French VAT**
 - **Use state-approved auctioneer**



NewsScan:

FTC TARGETS ONLINE AUCTION FRAUD

The Federal Trade Commission is launching an assault on online auction fraud, a problem that prompted 10,000 complaints last year, up from 107 in 1997. The agency plans to train law enforcement officers, educate the public and prosecute more offenders, but notes it lacks the jurisdiction to protect the rights of U.S. citizens who purchase items from overseas Web sites. Many online auction companies have responded by saying they will cooperate with FTC efforts: eBay, for example, will begin routing complaints about its vendors directly to the FTC this week. (Financial Times 15 Feb 2000)

<http://www.ft.com/>

* * *

FRENCH COURT SAYS "NON!" TO ONLINE AUCTIONS

A Paris court has barred French consumers from participating in online auctions unless they use a state-approved auctioneer and pay the French value-added tax. The ruling came in response to a lawsuit filed by the association of Paris auctioneers (commissaires priseurs) against online upstart Nart.com, the first company to auction off high-priced art work on the Net. Nart does not require its buyers to pay the tax, because its auctions are handled by a subsidiary incorporated in New York, with sales paid in U.S. dollars to a U.S. bank. The French court ruled the sales were illegal, because the activities were tantamount to the "organization of auctions of objects located in France." Nart says it will appeal the ruling: "This is almost like saying that French people should not be allowed to walk into Christie's or Sotheby's in New York and bid for something on sale there," says Nart co-founder Antoine Beaussant. (Financial Times 4 May 2000)

<http://www.ft.com/>

Online Auctions

2000-06: FBI investigates eBay shills

- Fraudulently raise auction prices
- CA lawyer started bidding on painting at \$0.25; reached \$135,805 (but no sale)
- eBay running proprietary "shill-hunter" software



NewsScan:

FBI INVESTIGATES AUCTION "SHILLING" ON EBAY

The Federal Bureau of Investigation has launched an investigation of several sellers in eBay auctions suspected of "shilling" (the practice of running up a bidding price through fraudulent bids by the seller or the seller's friends). The inquiry was prompted by a recent New York Times article about a California lawyer who almost sold an abstract painting for \$135,805, after starting the bid at 25 cents. Shilling is forbidden by eBay rules, and eBay is using its proprietary "shill hunter" software to review bidding by users. (New York Times 7 Jun 2000)

<http://partners.nytimes.com/library/tech/00/06/biztech/articles/07ebay-fraud.htm>

Online Auctions

2000-08: FBI & DoJ form IFCC

- **Internet Fraud Complaint Center**
- **Online auctions #1 reason for complaints**
- **Industry denies there's a problem**
 - **eBay claims only 1 in 40,000 auctions led to confirmed case of fraud**



NewsScan

INTERNET FRAUD

The Internet Fraud Complaint Center, a project of the FBI and the Department of Justice, says that online auctions are the No. 1 source of complaints about fraud on the Internet, and expects to receive more than 1,000 complaints a day starting in November when the center is fully automated. The online auction industry denies that fraud is a serious problem, and eBay says that only one of every 40,000 listings has resulted in a confirmed case of fraudulent activity. Complaints about Internet fraud can be reported to <http://www.ifccbi.gov>. (USA Today 29 Aug 2000)

<http://www.usatoday.com/life/cyber/tech/cti455.htm>

Online Auctions

2000-10: Yahoo provides insurance

- **Protect victims of fraudulent auctions, shopping**
- **Lloyd's of London**
- **"<1%" of all purchases on Yahoo are fraud**



NewsScan:

YAHOO PLANS PURCHASE PROTECTION INITIATIVE

Yahoo is launching a new program to protect consumers who make purchases made on its auction and shopping sites from fraud. The initiative, which is backed by insurance from Lloyd's of London, is designed to "add another layer of confidence for consumers during the shopping season," says Brian Fitzgerald, producer for Yahoo auctions, who adds that fraudulent transactions account for less than 1% of all purchases on the Yahoo commerce site. (AP/Los Angeles Times 16 Oct 2000)

<http://www.latimes.com/business/20001016/t000098573.html>

Hate Speech

2000-10: ADL releases

Online Guide to Hate Symbols

- **<http://www.adl.org>**
- **Catalog of hate-group symbols**
- **Alert communities to presence/growth of new hate groups**
- **Most symbols unknown to ordinary citizens**



NewsScan:

The Anti-Defamation League, www.adl.org, has created an online guide to hate symbols, logos, and tattoos to help people become aware of warning signs of the development of "hate" groups in their communities. A police official friendly to the ADL project says, "There are new symbols out there all the time. Unless you're affiliated with these groups, these are symbols you wouldn't have any idea about." (AP/New York Times 17 Oct 2000)

<http://partners.nytimes.com/aponline/nyregion/AP-Hate-Internet.html>

Impersonation

2000-02: President Clinton upstaged online

- **Christopher Petro / Lorcom Technologies**
- **Signed on as Pres.**
- **Wrote, "Personally, I would like to see more porn on the Internet."**
- **Nobody noticed anything odd ☺**
- **Claimed prank was harmless and was warning to CNN to beef up security**



NewsScan:

ONLINE PRANKSTER DISTORTS CLINTON CHAT

In what was billed as the first live online interview with a sitting U.S. president, CNN's chat with President Clinton turned kinky when a computer security consultant assumed Clinton's identity and changed his response to: "Personally, I would like to see more porn on the Internet." The consultant said guessing the president's nickname was an "easy trick," and that "I hope this harmless prank has served to let CNN know that this system is insecure and needs to be overhauled before someone does actual harm to them or one of their guests." Such security flaws can easily sabotage New Media journalism if not fixed, he added. (CBC News 16 Feb 2000)

<http://cbc.ca/cgi-bin/templates/NWview.cgi?/news/2000/02/15/online000215>

Impersonation

2000-06: domain names hijacked by forgery

- **Web.net & Bali.com lost DNS registration**
- **Forged e-mail from Jakarta to Network Solutions switched ownership of Web.net**
- **Forged e-mail from Madrid did same to Bali.com**



NewsScan:

DOT-COM NIGHTMARE -- DOMAIN NAME HIJACKING

At least two Internet companies recently suffered a dot-com's worst nightmare -- their domain names were reregistered without their knowledge, and all traces of their legal ownership were erased. Web.net, based in Toronto, and Bali.com of Hong Kong both have suffered crippling losses from the hijacking, which occurred last weekend. Sleuthing by Web.net's owners found that someone in Jakarta, Indonesia had sent a forged e-mail to Network Solutions, asking them to redirect all the site's e-mail and Web site information to a new location. He then requested that the registration, which had been recorded with Network Solutions in 1993, be transferred to a Toronto registrar, and asked them to switch the ownership to someone living in Hong Kong. In Bali.com's case, an investigation shows that the name now belongs to someone living in Madrid, Spain. "These are what I call A-class domain names," says Toronto Star columnist K.K. Campbell. "If the person collected 50 of these, they'd have \$5 million in assets they could afford to sit on for a little while until they're laundered and then resold." (Toronto Star 1 Jun 2000)

http://www.torontostar.com/editorial/updates/top/20000601NEW01d_CI-DOMAIN1.html

Identity Theft

2000-07: Kyle-Feinstein bill introduced in US Congress

- Credit-card issuers would have to confirm change of address with cardholder within 10 days
- Require conspicuous "fraud alerts" on credit reports once credit bureau notified of identity theft
- See <http://www.consumer.gov/idtheft>



MK:

Caitlin Liu of the Los Angeles Times published a thorough report on identity theft on January 16 (front page). In one case, 22-year-old San Diego college student Jessica Smith had her car stolen — with her handbag inside. Although the car and bag were recovered, someone stole her identity. She nearly got fired from her new job when a background check showed that "she" had outstanding warrants for prostitution. She was unable to obtain credit, phone service or even to rent an apartment. With the help of a sympathetic police investigator, Smith was able to prove her innocence of the charges — a reversal of the usual burden under criminal law, where usually the state has to prove guilt. She obtained judicial documents explaining that her identity had been stolen; nevertheless, she has been hauled into police stations to be fingerprinted to prove that she is indeed the person authorized to carry those documents.

Image Data LLC, an identity-fraud prevention service based in Nashua, NH, commissioned a study in September 1999 that suggested that one out of five Americans or a member of their family have been victimized by identity fraud. [Readers should always be wary of statistics that report how many "members of your family" or "people you know" have particular characteristics: it is possible that a single person can be reported by multiple people. The over-counting bias increases as a function of sample size and of social relationships among the sample population.]

* * *

NewsScan:

SENATE BILL TO PROTECT AGAINST IDENTITY THEFT

U.S. Senators Jon Kyl (R-Ariz.) and Diane Feinstein (D-Calif.) have introduced a bill to reduce the chances of identity theft, which Feinstein says "any thief with a computer can do anonymously," because "the Internet is making it very easy." The bill would require credit-card issuers to confirm any change of address with a cardholder within ten days, and would require "fraud alerts" to be conspicuously placed on credit reports once a consumer notifies a credit bureau of identity theft. The FTC site on identity theft is www.consumer.gov/idtheft/. (Washington Post 13 Jul 2000)

<http://www.washingtonpost.com/wp-dyn/articles/A31663-2000Jul12.html>

Law Enforcement Organizations, Cooperation

LawNet 2000-01

- **US Attorney General Janet Reno**
- **Information-sharing network**
 - **federal state local law-enforcement authorities**
- **Fight cybercrime**
 - **cybercrime laboratories**
- **Costs shared among participating agencies**
- **Speeding interstate transfers of subpoenas & warrants in Internet-related crime investigations**



CLINTON ADMINISTRATION BEEFS UP CYBERCRIME-FIGHTING EFFORTS

U.S. Attorney General Janet Reno is expected to announce today a proposal to create a national cybercrime-fighting network that will promote cooperation and coordination among law enforcement agencies, enabling them to respond quickly to crimes that often cross multiple jurisdictions in a matter of minutes. The proposal will include a new nationwide computer system for sharing investigative information on crimes ranging from hacking attacks to drug trafficking, and the creation of new forensic computer labs around the country staffed by personnel from federal, state and local law enforcement agencies. In addition, Reno will propose the formation of a network of specially trained computer crime coordinators at law enforcement agencies around the country who would be on call to respond computer-related crime.

(Los Angeles Times 10 Jan 2000)

<http://www.latimes.com/business/20000110/t000002956.html>

* * *

\$2 BILLION PLAN TARGETS TECH ATTACKS

President Clinton will release the first counter cyber-terrorism plan in the nation's history on Jan. 7, with the goal of ensuring that unfriendly governments and hackers cannot tamper with the nation's computerized infrastructure system. The \$2 billion plan was started in 1998, and the financing of the program is included in Clinton's fiscal 2001 budget, to be unveiled on Feb. 7. The program would raise the nation's funding for computer security research and development by 35 percent, to \$621 million. It would also create a Scholarships for Service program which would give 300 graduate and undergraduate scholarships annually to students who would then be required to work for the government for a certain amount of time after graduation. Training would be beefed up for the 5,000 to 10,000 government employees currently working in the field of information technology security. The program would also establish the Institute for Information Infrastructure Protection, which would create joint ventures between the government and private companies on security research. (USA Today, 7 Jan 2000)

Law Enforcement Organizations, Cooperation

2000-01: UK Strawman Proposal

- British Home Secretary Jack Straw
- National computer-crime squad
 - part of National Criminal Intelligence Service (NCIS)
- Develop specialized team to attack Internet crimes: fraud, money laundering, pornography, illegal gambling, pedophile rings
- Collaborate with other agencies
 - taxation department (Inland Revenue)
 - domestic security intelligence (MI5)
 - international surveillance center (GCHQ)



POLICE GO TO WORK ON NET CRIME.

By Linus Gregoriadis.

Jack Straw is backing plans for a national squad to tackle escalating computer crime, the Home Office said last night.

The Home Secretary has asked a chief constable and the National Criminal Intelligence Service (NCIS) to draw up plans for a unit to deal with "cyber criminals" who commit fraud and launder money on the Internet. Mr Straw has told the NCIS that it must spend £337,000 of its annual budget on the national computer crime squad. He has indicated that the service will receive a 14 per cent rise in funding to cope with the new demand, according to an NCIS spokesman.

The squad, which will be assisted by the Inland Revenue, MI5 and GCHQ, the Government's spying centre, will also try to combat "hate sites", illegal gambling, pornography and paedophiles who share information on the net.

Roger Gaspar, Director of Intelligence at NCIS, and David Phillips, Chief Constable of Kent, have been planning the squad since it was recommended by the NCIS last summer.

It is believed that the squad will operate from the NCIS headquarters in London, with a separate wing at Scotland Yard. The NCIS is liaising with computer experts at the National Security Agency, the US intelligence organisation.

(c) Times Newspapers Ltd, 2000.

THE TIMES 17/01/2000 P4

Law Enforcement Organizations, Cooperation

2000-02: Clinton Increases Budget for CALEA

- **Clinton administration proposed a \$1.84T budget fiscal 2001**
- **Would include major increases in spending on law enforcement capabilities**
 - **E.g., wiretapping**
- **Reimburse telcos \$240M (up from \$15M)**
 - **Controversial CALEA (Communications Assistance to Law Enforcement Act)**
 - **Rewiring networks to make wiretapping easier**



In February, the Clinton administration proposed a \$1.84T budget fiscal 2001 that would include major increases in spending on law enforcement capabilities such as wiretapping. The government would reimburse telcos to the tune of \$240M (up from \$15M) under the controversial CALEA (Communications Assistance to Law Enforcement Act) for rewiring their networks to make wiretapping easier.

[However, in August (wrote the NewsScan editors), A three-judge panel of the U.S. Court of Appeals for the District of Columbia . . . ruled that the Federal Communication Commission's attempts to implement a 1994 electronic wiretap law have been too accommodating to law enforcement agencies and not sufficiently protective of the right of citizens to individual privacy or of the financial requirements of companies. The wiretap law (the Communications Assistance for Law Enforcement, or CALEA) was passed by Congress because the FBI had insisted it was losing ground against criminals because wireless phone companies were not designing wiretapping capabilities into their networks. An executive of the Center for Democracy and Technology, which had opposed the FBI's request to Congress, . . . [said] the appellate court's decision means that "government cannot get its hands on what it's not authorized to get just by promising it won't read what it's not supposed to read." (Washington Post 16 Aug 2000)

* * *

See also

Wired <<http://www.wired.com/news/politics/0,1283,34164,00.html> > ,

Washington Post <<http://www.washingtonpost.com/wp-dyn/articles/A32193-2000Aug15.html> >

Law Enforcement Organizations, Cooperation

2000-02: EC Attacks Cybercrime

- **European Commission**
- **Process for improving battle against cybercrime**
- **Considering special school for law enforcement**
 - **learn more about fighting cyberspace crime**
- **Increased involvement by Interpol**
 - **criminal investigations involving computers and networks**



EU TO ACT ON 'CYBERVILLAINS'.

By ANNAMARIE CUMISKEY.

Brussels is 'urgent' in its war on online crooks, reports Annamarie Cumiskey.

Recent attacks on major websites have encouraged the European Commission to put together an action plan. An EU spokesman said: "The attacks have served to focus attention on cybercrime and created a sense of urgency to address them. "The commission will do its utmost to accelerate progress in this field."

The EU fears that hackers will be driven to carry out more attacks because of the publicity surrounding their recent successes. It is also concerned that the number of European criminals using the anonymity of the Web to communicate is on the increase. The Web is also a useful tool for credit card fraud, money laundering and running illegal child pornography rings.

EU officials are sounding out the opinions of national governments on plans to combat cybercrime. These will be made public in the summer.

One solution, the commission believes, would be to set up a police school to teach officers how to identify internet crimes and track down online criminals. Another possible solution involves Interpol, which currently exchanges information about criminals between national police forces. The commission would like it to co-ordinate online investigations managed by national police. The commission realises that criminals can move swiftly in cyberspace, covering their tracks as they go and staying out of reach. It wants national police to work closely with internet providers in tracking criminals online.

Funding will also be available under the commission's IST research programme to develop technology suited to online police investigations, such as software for decoding encryption. In addition, the commission aims to make companies and individuals more aware of how to protect themselves against security attacks.

(c) Telegraph Group Limited, London, 2000.

DAILY TELEGRAPH 17/02/2000 P3

Law Enforcement Organizations, Cooperation

2000-02: SEC Fights Cyberfraud

- **Securities Exchange Commission (SEC)**
- **100 new officials fight cyberspace fraud**
- **60 to police Web**
- **Already 250 workers scanning Web full time**
- **"Frightening" recent case**
 - **criminal hacker inserted false news re merger of company on Web site**
- **Stock manipulations include rumor-mongering:**
 - **drive up price stock already held**
 - **drive down price stocks already sold on margin**



SEC HIRING CYBERCOPS TO POLICE INTERNET.

By Sherman Fridman, Newsbytes. – 18 Feb 2000

Securities and Exchange Commission (SEC) Chairman, Arthur Levitt, is out to wage war against Internet fraud, and he's hiring the some virtual gumshoes to help him do it. According to a published report in Reuters today, the SEC has already hired half of its desired goal of some 60 new cybercops to ride herd on the "lawlessness," which Levitt believes exists on the World Wide Web.

Following last week's hacker attacks on several popular Web sites, Levitt reportedly indicated that the SEC plans to add up to 100 people to its 850-member enforcement staff. This enforcement staff is made up primarily of lawyers and analysts, with about 60 of them dedicated to combating what is being described as "burgeoning Internet fraud." According to Richard Walker, SEC enforcement director, "The ease of spreading false information via e-mail, chat rooms, and Web sites has made the Internet fertile ground for stock fraud."

Officials at the SEC are reported to have said that the Internet has become an extraordinary efficient and cheap method of conducting stock frauds that used to be the domain of old-fashioned "boiler rooms" and other scams.

The SEC is said to have a cyberforce of some 250 investigators who spend part of their time surfing the Web looking for fraud. Walker cited what he called a "frightening" case, which came to light this past week, in which someone hacked into the Web site of a publicly traded company and posted a false notice announcing a merger with another company. "We've got to locate the hackers and bring them to justice," Walker said.

Of particular concern to the SEC are the so-called "momentum" sites, where investors are urged to buy a certain stock at a specific time in order to build momentum to drive up the price of the stock, and "cybersmears," in which negative news about a company is disseminated on the Internet in an effort to drive down its stock price in order to enrich sellers who have sold stock they didn't have in hopes of buying it at a lower price in time to transfer it to the new owners.

Reported by Newsbytes.com, <http://www.newsbytes.com>. -- 16:38 CST.
Newsbytes News Network, Copyright 2000.

Law Enforcement Organizations, Cooperation

2000-03: FTC announces intl cooperation

- **Sweep of 1,600 suspected Web sites in 28 countries**
- **Pyramid schemes, unrealistic investments, easy-money**



NewsScan:

FTC SWEEP TARGETS 1,600 "GET-RICH-QUICK" SITES

The U.S. Federal Trade Commission says it's been working with other international organizations in an unprecedented global effort to crack down on fraudulent, get-rich-quick schemes that are promoted through the Internet. The sweep, which began in February, involved 28 countries and targeted 1,600 suspect Web sites. Typical scams included pyramid schemes, unrealistic investment opportunities and easy-money come-ons. Domestically, the FTC has enlisted the help of the Postal Service and the Securities and Exchange Commission enforcement units to assist in monitoring online fraud. FTC officials say the sites have now been warned that they must change their claims or it will attempt to have them shut down. "We're going to run them off the Web and where appropriate, put them in jail," says Drew Edmondson, attorney general of Oklahoma. (Financial Times 24 Mar 2000)

<http://www.ft.com/>

Law Enforcement Organizations, Cooperation

**2000-09: US e-commerce merchants, payers
combine to fight e-fraud**

- **Merchants must pay for fraud — U\$9B/year by 2001**
- **Worldwide E-Commerce Fraud Prevention Network**
- **AMEX, Buy.com, Expedia. . .**
- **Clearinghouse for fraud-prevention information**



NewsScan:

E-COMMERCE COMPANIES TACKLE ONLINE FRAUD

A group of leading U.S. e-commerce merchants and payment processing companies have formed an industry coalition to reduce online fraud. The Worldwide E-Commerce Fraud Prevention Network, which includes American Express, Buy.com and Expedia, will serve as a clearinghouse for information on best fraud prevention practices and current fraud prevention trends, as well as security seminars, law enforcement resources and security software vendors. One of the main concerns for members is that online merchants are often held liable for the cost of goods purchased with stolen credit cards. "More than 41% of the merchants we canvassed didn't know that they -- not the credit card companies -- are liable for fraud," says one security software firm executive. "Online credit card fraud is projected to cost merchants US\$9 billion annually by next year." (E-Commerce Times 26 Sep 2000)

<http://www.ecommercetimes.com/news/articles2000/000926-3.shtml>

Law Enforcement Technology

- 2000-07: FBI Carnivore ISP e-mail sniffer
 - High-speed
 - Used in <100 cases
 - Can target single user among millions
 - Used only with warrant
 - Privacy advocates going ballistic
- 2000-08: Fed judge orders FOIA cooperation
 - ACLU & EPIC demand access to records
 - AG Reno orders choice of US university for review of Carnivore
- 2000-09: Vincent Cerf satisfied about privacy under Carnivore
- 2000-09: NetICE develops Altivore (free) to replace Carnivore & protect privacy better

100



NewsScan:

'CARNIVORE' HAS PRIVACY ADVOCATES GNASHING TEETH

The Federal Bureau of Investigation is using a superfast e-mail-surveillance software system called Carnivore, so named because it can quickly ferret out "the meat" among a vast quantity of data in search of criminal or terrorist content. FBI investigators say the Internet wiretapping system has been used in fewer than 100 criminal cases since its launch last year, but privacy advocates say its deployment gives government, at least theoretically, the ability to eavesdrop on all customers' digital communications, from e-mail to online banking to Web surfing. The FBI defends Carnivore as more precise than the primitive Internet wiretap systems used in the past, and credits it with the ability to target the digital traffic of just one user amidst a stream of millions of other messages. "This is just a very specialized sniffer," says Marcus Thomas, head of the FBI's Cyber Technology Section, but Republican Congressman Bob Barr (R-Ga.) counters, "Once the software is applied to the ISP, there's no check on the system. If there's one word I would use to describe this, it would be 'frightening.'" (Wall Street Journal 11 Jul 2000)

<http://interactive.wsj.com/articles/SB963264584706292829.htm>

* * *

FBI DEFENDS INTERNET SURVEILLANCE SYSTEM

In testimony before a House Judiciary subcommittee, FBI official Donald M. Kerr strongly defended the agency's use of the "Carnivore" system, which effectively places a wiretap on the Internet and allows law enforcement officials to identify the origin and destination of all e-mail messages related to a person under suspicion of a crime. The reaction of Rep. Spencer Bachus (R-Ala.) was skeptical: "The potential for abuse here is tremendous. What you're saying is 'Trust us.'" But Kerr insisted that Carnivore was an essential tool for fighting crime: "Criminals use computers to send child pornography to each other using anonymous, encrypted communications. Hackers break into financial service companies' systems and steal customers' home addresses and credit-card numbers, criminals use the Internet's inexpensive and easy communications to commit large-scale fraud on victims all over the world, and terrorist bombers plan their strikes using the Internet." Civil liberties groups have been consistently critical of the FBI's support of Carnivore. (Washington Post 25 Jul 2000)

<http://www.washingtonpost.com/wp-dyn/articles/A36665-2000Jul24.html>

Law Enforcement Technology

1D2

- **2000-10: Judge pines for evanescence**
 - **NY District Judge James Rosenblum**
 - **“In Defense of the DELETE Key”**
 - **Wishes people would delete their e-mail, notes to preclude use in litigation**
 - **“cyber statute of limitations” (e.g., 6 mo.)**
 - **Electronic documents would no longer be usable as evidence**
 - **Exceptions allowable**

101



NewsScan:

JUDGE MAKES A CASE FOR THE DELETE KEY

District Court Judge James Rosenbaum has published an article called "In Defense of the DELETE Key," in which he bemoans the eternal nature of computer communications and reminisces fondly about pre-computer days when people casually spoke "off the record": "At this earlier time, two people could easily say something -- even, perhaps, something politically incorrect -- simply between themselves. They might even have exchanged nasty notes between themselves. And when they had moved past this tacky, but probably innocent moment, it was truly gone." Today, however, "an idle thought jotted onto a calendar, a tasteless joke passed to a once-trusted friend, a suggestive invitation directed at an uninterested recipient, if done electronically, will last forever. Years later, it can subject its author to liability." Rosenbaum proposes a "cyber statute of limitations" -- perhaps six months for an isolated e-mail message -- after which "deleted" documents would be legally consigned to the electronic rubbish heap and become inadmissible as evidence of possible wrongdoing. He makes an exception for recovered "deleted" messages from someone who has exhibited a pattern of egregious behavior or communications. The article was published in the Summer issue of *The Green Bag*, a literary law journal. (New York Times 5 Oct 2000)

<http://.nytimes.partners.com/2000/10/05/technology/06CYBERLAW.html>

Law Enforcement Technology

2000-10: NeoTrace used to trap porn fraudsters

- Tricked customers into paying \$4/minute for dialup access to porn “from Madagascar”
- Actually calls went to UK; cost \$0.08/minute
- Overcharges averaged \$222 (some >\$4,000)
- FTC used COTS NeoTrace (from Networx) to find porn merchants
- Software identifies geographic origin of calls
- Used by FBI, US Customs, NATO, RCMP, Interpol



FTC CHARGES GLOBAL PORN RING WITH PHONE FRAUD

The Federal Trade Commission filed a complaint in federal court Thursday alleging that Verity International, which is registered in Dublin and is no relation to the California software company Verity Inc., improperly charged thousands of U.S. Internet users for long-distance phone calls. The porn customers were told they were being charged to view sex videos over a phone line to Madagascar at a rate of \$3.99 a minute, but the FTC determined that the calls actually terminated in the U.K. and should have cost only eight cents a minute. Verity planned to pocket the difference. The scope of the scam was huge -- in a single week in September, some 67,000 U.S. households received bills from Verity, with an average overcharge of \$222 (although some overcharges topped \$4,000). Interestingly, the agency used an off-the-shelf software program called NeoTrace to locate the alleged perpetrators. According to NeoTrace's manufacturer, NetWorx, the software is used by the FBI, the U.S. Customs Service, NATO, the Royal Canadian Mounted Police and Interpol to trace the geographic origin of Internet traffic. (Wall Street Journal 6 Oct 2000)

<http://interactive.wsj.com/articles/SB970787581170382228.htm>

Law Enforcement Technology

2000-12: Confusion over legality of pen traps for e-mail/Internet messaging

- 1986 ECPA (Electronic Communications Privacy Act) controls access to e-mail
- LEO allowed to record *phone numbers* when warrant allows tap on *phone lines*
- Interpreted to mean OK to trap e-mail addresses when subject under wiretap
- Questionable: e-mail address not a phone number and Carnivore does not intercept phone line



NewsScan:

Law enforcement officials have long held that a 1986 law allowing police to record phone numbers by someone tied to a criminal investigation permits them to secretly copy e-mail addresses in messages sent to people involved in criminal probes, but a newly disclosed e-mail message suggests there is internal dissension over the legality of such "pen traps": "We have agents that would like to use a pen for e-mail, but our [chief division counsel] thinks that we can only use a pen to get the telephone number dialed by the modem," one agent wrote in the Feb. 14 e-mail. "I don't think we in the field have a grasp of how the existing telecommunications laws apply to computer communications." Highlighting the depth of confusion over the issue within law-enforcement circles, the agent noted that this legal opinion came from the FBI's National Infrastructure Protection Center, which includes the bureau's top computer-crime experts in Washington. The uncertainty brings into question the legality of using Carnivore, the FBI's e-mail "sniffing" software, which has been justified under the 1986 law that covers any device that "records or decodes electronic or other impulses, which identify the numbers dialed or otherwise transmitted" and that is attached to a telephone line. "Carnivore is not attached to a telephone line and does not obtain a number dialed," says Philip L. Gordon, a lawyer with the Privacy Foundation, who notes that privacy protections for e-mail addresses should be greater than those for phone numbers. "They're clearly different." (Wall Street Journal 7 Dec 2000)

Litigation, Legal Rulings, Judgements

**2000-01: Spokane County, WA rejects 1st
amend protection of e-mail**

- **Rape/child porn trial**
- **Defense argued that captured e-mail should
be excluded evidence**
- **Judge ruled evidence admissible**



NewsScan:

CYBERPRIVACY ISSUE IN STATE OF WASHINGTON

A Washington state judge has ruled that state privacy laws preventing your phone conversations from being recorded without your permission do not apply to e-mail messages or online chats. The issue arose when public defense attorneys in a rape and child pornography trial argued that prosecutors could not use evidence the police offered in printouts of the defendant's e-mail messages or his banter in an online chat group. Judge Kathleen M. O'Connor of Spokane County Superior Court ruled, however, ruled against the defense motion, on the grounds that the statute does not specifically mention computers as a covered device. Commenting on the case, Gonzaga University law professor Jeffrey K. Finer distinguishes between e-mail and chat, saying that the writer of an e-mail message is implicitly consenting to its recording (since e-mail messages have to be stored on a hard drive), but chat messages may or may not be recorded and are more like "a spontaneous, back-and-forth, written conversation, like a private conversation at a party. That's exactly the kind of private conversation the privacy law in Washington was designed to protect -- spontaneous utterances that are nobody's business." (New York Times Cyber Law Journal 14 Jan 2000)

<http://www.nytimes.com/library/tech/00/01/cyber/cyberlaw/14law.html>

Litigation, Legal Rulings, Judgements

**2000-02: UK House of Lords denies warrantless
log files**

- **Stephen Alan Morgans convicted of
phreaking**
- **Log files from wiretap placed without warrant**

105



MK:

In England, the House of Lords ruled in favor of Stephen Alan Morgans, who appealed a conviction based in part on log files printed out from a device placed on the defendant's telephone line. The printouts showed that Mr Morgans had accessed phone company computers and fraudulently obtained phone services. Unfortunately, police had failed to obtain a warrant from the office of the Secretary of State. The Lords threw out the conviction on the grounds that the intercepts were illegal.

Litigation, Legal Rulings, Judgements

2000-07: Entrapment via e-mail ruled inadmissible

- Undercover police investigator suggested child rape
- Man arrested when he showed up
- Evidence showed no prior evidence whatever of pedophilia
- US Appellate Court threw out charges



NewsScan:

COURT RULES AGAINST POLICE IN INTERNET "ENTRAPMENT" CASE

A majority of a three-judge U.S. appellate court panel has ruled against the use of the Internet to entrap an individual into committing sex offenses. After being divorced by his wife because he could not control his compulsion to cross-dress, the individual in question began to use the Internet to search for a woman who would accommodate his sexual tastes. He entered into correspondence with someone called Sharon, who turned out to be an undercover police investigator, who suggested the idea of having sex acts with her children. The man was arrested when he showed up at a meeting place to carry out the plan. The court ruled: "Prior to his unfortunate encounter with Sharon, [the man charged for attempting to have sex with minors] was on a quest for an adult relationship with a woman who would understand and accept his proclivities, which did not include sex with children. There is surely enough real crime in our society that it is unnecessary for our law enforcement officials to spend months luring an obviously lonely and confused individual to cross the line between fantasy and criminality." (New York Times 7 Jul 2000)

<http://partners.nytimes.com/library/tech/00/07/cyber/cyberlaw/07law.html>

Government Funding

- **2000-02: Clinton Administration proposes \$1.84T budget**
 - **Fiscal 2001**
 - **Major increase in LE facilities for wiretapping**
 - **Reimbursement for ISPs under CALEA (Communications Assistance to Law Enforcement) legislation**
- **2000-08: US Court of Appeals for DC rules against CALEA**
 - **Ruled that FCC excessively accommodating to law enforcement**
 - **Not sufficiently protective of citizen privacy rights**



In February, the Clinton administration proposed a \$1.84T budget fiscal 2001 that would include major increases in spending on law enforcement capabilities such as wiretapping. The government would reimburse telcos to the tune of \$240M (up from \$15M) under the controversial CALEA (Communications Assistance to Law Enforcement Act) for rewiring their networks to make wiretapping easier.

[However, in August (wrote the NewsScan editors), A three-judge panel of the U.S. Court of Appeals for the District of Columbia . . . ruled that the Federal Communication Commission's attempts to implement a 1994 electronic wiretap law have been too accommodating to law enforcement agencies and not sufficiently protective of the right of citizens to individual privacy or of the financial requirements of companies. The wiretap law (the Communications Assistance for Law Enforcement, or CALEA) was passed by Congress because the FBI had insisted it was losing ground against criminals because wireless phone companies were not designing wiretapping capabilities into their networks. An executive of the Center for Democracy and Technology, which had opposed the FBI's request to Congress, . . . [said] the appellate court's decision means that "government cannot get its hands on what it's not authorized to get just by promising it won't read what it's not supposed to read." (Washington Post 16 Aug 2000)

* * *

See also

Wired <<http://www.wired.com/news/politics/0,1283,34164,00.html> >

Washington Post <<http://www.washingtonpost.com/wp-dyn/articles/A32193-2000Aug15.html> >

Ideas

- **Organize endowed chairs for universities in INFOSEC**
 - Professional IT & security associations
 - Business groups
- **Counter criminal-hacker propaganda**
 - Discuss issues in schools, community groups, religious organizations
 - Use “Why Kids Shouldn’t Be Criminal Hackers” from KFILES
 - www.securityportal.com



DISCUSSION

109

