M. E. Kabay, PhD, CISSP
Assoc. Prof. Information Assurance
Dept. of Computer Information Systems, Division of Business
Norwich University

mkabay@norwich.edu

# 11.1 Data leakage

Category 11.1 Data leakage

2002-02-20 search engine spider web-bot exclusion cache

RISKS 21 92

RISKS correspondent Diomidis Spinellis cogently summarized some of the problems caused by search engines on the Web: "The aggressive indexing of the Google search engine combined with the on-line caching of the pages in the form they had when they were indexed, is resulting in some perverse situations.

A number of RISKS articles have already described how sensitive data or supposedly non-accessible pages leaked from an organization's intranet or web-site to the world by getting indexed by Google or other search engines. Such problems can be avoided by not placing private information on a publicly accessible web site, or by employing metadata such as the robot exclusion standard to inform the various web-crawling spiders that specific contents are not to be indexed. Of course, adherence to the robot exclusion standard is left to the discretion of the individual spiders, so the second option should only be used for advisory purposes and not to protect sensitive data."

Category 11.1 Data leakage

2002-03-22 design QA quality assurance confidentiality Web URL

RISKS 22

Paul van Keep reported in RISKS, >Christine Le Duc, a dutch chain of s\*xshops, and also a mail & Internet order company, suffered a major embarrassment last weekend. A journalist who was searching for information on the company found a link on Google that took him to a page on the Web site with a past order for a CLD customer. He used the link in a story for online newspaper nu.nl. The full order information including name and shipping address was available for public viewing. To make things even worse it turned out that the classic URL twiddling trick, a risk we've seen over and over again, allowed access to ALL orders for all customers from 2001 and 2002. The company did the only decent thing as soon as they were informed of the problem and took down the whole site.<

http://nu.nl/document?n=53855

[Note: \* included to foil false positive exclusion by crude spam filters.]

Category 11.1 Data leakage

2002-06-10 QA quality assurance Web confidentiality breach customer activity

RISKS; http://www.msnbc.com/news/758979.asp

22 12

Monty Solomon wrote in RISKS, "A design flaw at a Fidelity Investments online service accessible to 300,000 people allowed Canadian account holders to view other customers' account activity. The problem was discovered over the weekend by Ian Allen, a computer studies professor at Algonquin College in Ottawa. Fidelity said it had fixed the problem and was offering customers the option of changing account numbers."

# 11.2 Unauthorized disclosure

Category 11.2 Unauthorized disclosure

2002-04-25 confidential personal data storage credit card identity theft error investigation

mystery

Security Wire Digest 4 32

#### TOPEKA OFFICIALS STUMPED BY FILE FOUND ON WEB SITE

Topeka officials have removed a file containing personal and financial data from its official city Web site after learning the file was accessed over the Internet. Though a user would need to know the exact file name and location on a particular computer, a Washington man says he accessed the information and then contacted a local newspaper in Kansas. Using a Web browser, the man found a file listing addresses, phone numbers and, in several dozen cases, credit card numbers for participants in city recreation department programs. Officials speculate the file may have erroneously landed in the computer hosting the site during a file transfer from one computer to another as long ago as January 2000.

Category 11.2 Unauthorized disclosure

2002-05-08 console log confidentiality audit trail documentation server risk management

RISKS 22 06ff

Mark Bergman noted in RISKS that he was surprised at the detail and length of the console log record kept by a diagnostic service processor on a server; it included full details of remote reconfiguration sessions. Mr Bergman warned everyone to be aware of just how detailed an audit trail any network device keeps so that appropriate security can be imposed.

Category 11.2 Unauthorized disclosure

2002-11-21 data leakage unauthorized disclosure costs prices consumers marketing

NewsScan

#### WEB SITES LEAK AFTER-HOLIDAY SALE PRICES

Users of several shopping Web sites, including FatWallet.com and DealofDay.com, were treated to a sneak peek of post-Thanksgiving sale prices for items ranging from Kodak digital cameras to the "8 Mile" movie soundtrack -- prices retailers had no intention of revealing until after the holiday. Now, shoppers in the market for an HP printer may as well wait until the price drops to \$200 after Thanksgiving -- 33% off the current price on the OfficeMax Web site. And Best Buy's price on a digital camera will drop to \$99.99 from its current \$149.99 listing. "Someone, somewhere is getting information they shouldn't be," says an OfficeMax spokesman. Target, Best Buy, Wal-Mart, Toys R Us and others have demanded that the Web sites take the information down. Most have complied, but in many cases readers have already copied the data and posted it elsewhere on the Web. Retailers are stumped over how the information got out, but promise to take retaliatory action when they find out: "We will take appropriate legal action as soon as we discover how the information got on the site and who posted it," says a spokesman for OfficeMax. (Wall Street Journal 21 Nov 2002)

# 11.3 Data theft

Category 11.3 Data theft

2002-05-23 penetration confidentiality data theft credit reports

RISKS 22 09ff

According to a story excerpted in RISKS by Dave Hansen, >Officials still aren't sure who, or how, someone snatched 13,000 credit reports through Ford Motor Credit Co.'s Grand Rapids office." What they are sure about, however, is that no more credit reports will be stolen -- at least from this group. "We're not sure how this happened, to be honest," said Melinda Wilson, spokeswoman for Ford Motor Credit. "We thought we had a tight system. We're going to have an even tighter system now." The reports provided the intruders with a wealth of information, such as Social Security numbers, credit ratings, account numbers for bank accounts and credit cards, and creditors names and payment histories, Experian said. Hansen commented, "Apparently, someone was able to steal credit reports from Experian by masquerading as Ford Motor Credit. They don't know how, but it won't happen again. Very confidence inspiring...."

Category 11.3 Data theft

2002-09-12 penetration data theft employee spam

NewsScan

#### LYRIS LISTS TARGETED FOR SPAM

Lyris Technologies, an e-mail list management company, says it's received reports that some of its customers' mailing lists may have been compromised. The company says it's looking into spam complaints that may involved hundreds of thousands of list subscribers, and has hired an outside consulting firm to sort through the evidence. It's also investigating whether a disgruntled employee might have stolen its lists. "In the envelope world of marketing, lists are routinely stolen by employees that are moving to another company," says Jason Catlett, president of Junkbusters, who notes that spammers especially covet lists of validated e-mail addresses belonging to a targeted group. "I don't have any evidence that that happened in this case, but it's happened in the offline world, and it wouldn't be implausible if it happened online." (CNet News.com 11 Sep 2002) http://news.com.com/2100-1023-957567.html?tag=fd\_top

# 11.4 Covert channels

Category 11.4

Covert channels

2002-03-07

covert channel eavedropping interception surveilliance privacy information warfare confidentiality

NewsScan, RISKS 21 95FF

#### LED LIGHTS CAN REVEAL COMPUTER DATA

Scientists in the U.S. and the U.K. have found a way to remotely eavesdrop on a computer by monitoring the flashes of LED lights on electronic devices. Optical signals from the light-emitting diode lights found in computer modems and keyboards can be captured with a telescope and processed to reveal all the data passing through the device, says Joe Loughry, a computer programmer at Lockheed Martin. "It requires little apparatus, can be done at a considerable distance, and is completely undetectable. In effect, LED indicators act as little free-space optical data transmitters, like fiber optics without the fiber." Loughry says the most vulnerable devices are equipment used in low-speed, long-distance networks, such as ATMs (automatic teller machines). Corporate LANs and home Internet connections are generally not susceptible to the spying technique. Loughry says his interest in LEDs dates back to his days in graduate school: "I was working very late one night and waiting for a long file transfer to complete and I was just staring at these lights on the front of the modem and started to wonder if there was anything there." Loughry recommends locating equipment away from windows, putting black tape over the LEDs or deactivating when not in use. (Reuters 7 Mar 2002)

http://story.news.yahoo.com/news?tmpl=story&cid=581&u=/nm/20020307/tc\_nm/tech\_snooping\_dc\_1

\* \* \*

A vigorous discussion in RISKS poured scorn on the notion that data could be read at any but very slow transfer rates from LEDs; correspondents noted that LEDs have a long persistence phase that would grossly swamp the fluctuations of any but glacially slow transfers. Commentators relegated the claims to the FUD (fear, uncertainty and doubt) bin and recalled seeing similar discussions in the alt folklore computers USENET group. on the other hand, some correspondents did recount personal involvement in successful data transfer experiments using diodes and light pens that were used for debugging systems.

Category 11.4 Covert channels

2002-03-18 photocopier memory confidentiality data leakage

RISKS 22 01

Alistair McDonald noted in RISKS that some modern photocopiers scan documents into memory and hold the image until paper is available. The next time someone replaces the paper, the stored image(s) get printed -- even if the person who wanted them copied has gone away. Such situations could compromise confidentiality. MORAL #1: don't assume that you know how unfamiliar machines work -- find out the details if you care about the possible consequences. MORAL #2: when designing systems, provide alerts to inform users of threats to their security. An indicator labeled "IMAGE CURRENTLY IN MEMORY" would have been nice.

# 12.1 Wiretapping

Category 12.1

Wiretapping

2002-06-11

surveillance bugging eavedropping countermeasure detection wireless bugsweepers

NewsScan

#### DETECTING CELL PHONES USED AS BUGGING DEVICES

An Israeli company has developed a device that can detect when a room is being bugged by a modified cell phone, which an intruder could call from anywhere in the world without it emitting a ringing tone. The phone's screen remains blank and it appears to be turned off. A co-designer of the device says, "The beauty of the cell phone as a bug is that it's an innocent looking and ubiquitous object. People trust cell phones, but modified and left in idle mode the cell phone can be used as a transmitter for up to a week. If it's connected to a power supply it can provide endless intelligence. Professional bugsweepers will ignore the cell phone frequency since the phones are so common and not suspicious." (Reuters 11 Jun 2002) http://story.news.yahoo.com/news?tmpl=story&cid=581&ncid=581&e=4&u=/nm/20020611/tc\_nm/tech\_israel\_netline\_dc\_1

# 12.2 Interception

Category 12.2 Interception

2002-01-24 ISP Internet service provider credit-card fraud snooping e-mail interception

accusation trial prosecution

RISKS 21 89

In Brisbane, Australia (reports Peter Deighan in RISKS), the Australian Competition and Consumer Commission began legal proceedings against the owners of an Internet service provider called Dataline.net.au for allegedly intercepting e-mails, collecting credit-card numbers, and debiting customers' credit cards without authorization. http://203.6.251.7/accc.internet/digest/view\_media.cfm?RecordID=574

Category 12.2 Interception

2002-02-11 hotel Internet access proxy rerouting undocumented cache snooping interception

confidentiality profiling SMTP server e-mail

RISKS 21 91

Christian Holz discovered that the "STSN Internet Access, common at hotels.... re-route packets based on the service used(!)." Specifically, when he tried to reach his own SMTP server, he found that in fact his traffic was being rerouted -- without notification or permission -- to STSN's SMTP server. He concluded, "The risk: Obvious, if they can re-direct based on the service used, they could possibly see a lot of passwords by providing proxy-services for common services. In addition with the hotel-guest information, this could give an interesting profile of hotel guests. I wonder what information they can get their hands on if they have this services in Capitol-Hill hotels."

Category 12.2 Interception

2002-02-20 eavesdropping interception spying confidentiality government law privacy

surveillance politics information warfare

RISKS 21 92

According to RISKS correspondent Geoffrey Bent, the government of Australia has admitted that there were violations of the Australian rules forbidding the Defence Signals Directorate from intercepting Australian communications during the notorious "Tampa" affair in which refugees picked up by that ship were the subject of intense political debate which was thought to have altered the political fortunes of the government.

Category 12.2 Interception

2002-03-12 data leakage covert channel physical access telephoto lens

Boston Globe http://digitalmass.boston.com/news/2002/03/12/data\_leak.html

Two computer scientists were able to intercept data being transmitted via modems, routers and other electronic equipment with light-emitting diodes (LEDs) that blink as a function of data flow. Joe Loughry works at Lokheed Martin Space Systems in Denver, CO; David Umphress is Assoc. Prof. Computer Science at Auburn University in Alabama. Using a 100 mm focallength lens coupled to a sensitive light detector, they were able to decode transmitted data at a distance of up to 100 feet (~33 m). In a related piece of research, it appears that Markus Kuhn at Canbridge University has worked out how to read daa from computer screens by analyzing the light reflected from the surrounding walls. Recommendations: move flashing lights away from windows; use duct tape to mask the lights.

Category 12.2 Interception

2002-06-27 satellite confidential cleartext Internet

RISKS, http://www.guardian.co.uk/international/story/0,3604,736462,00.html 22

Duncan Campbell, writing in \_The Guardian\_ (June 13, 2002):

European satellite TV viewers can watch live broadcasts of peacekeeping and anti-terrorist operations being conducted by US spyplanes over the Balkans. Normally secret video links from the American spies-in-the-sky have a serious security problem - a problem that makes it easier for terrorists to tune in to live video of US intelligence activity than to get Disney cartoons or new-release movies. For more than six months live pictures from manned spy aircraft and drones have been broadcast through a satellite over Brazil. The satellite, Telstar 11, is a commercial TV relay. The US spyplane broadcasts are not encrypted, meaning that anyone in the region with a normal satellite TV receiver can watch surveillance operations as they happen. The satellite feeds have also been connected to the Internet, potentially allowing the missions to be watched from around the globe.

13

Category 12.2 Interception

2002-11-08 wireless keyboard data leakage confidentiality eavedropping

NewsScan

#### TYPE ONCE, READ MANY PLACES

Two men in Norway recently made headlines when they discovered that the text one of them was typing on his Hewlett-Packard cordless keyboard was also appearing on a neighbor's computer in another building at least 150 meters away. They have since had their equipment replaced, but the problem persists and HP Norway product manager Tore A. Särelind says the firm is taking it "deadly seriously," and has mobilized forces to correct the situation. "Among other things we will check the suitability of the frequency we use. It is a so-called walkie-talkie frequency with a radius that can be difficult to limit," says Särelind. "We would also like to do an 'on-site' test in the area where Helle and Evjeberg live to see if there are special circumstances there which might influence the reach of the keyboards." Over 65,000 of the keyboards have been sold in Europe. (Aftenposten 6 Nov 2002)

http://www.aftenposten.no/english/local/article.jhtml

# 13.2 Data corruption & destruction

Category 13.2 Data corruption & destruction

2002-01-15 data destruction sabotage evidence recovery forensic analysis reconstruction e-mail

files data investigation

NewsScan

#### DATA-RECOVERY EXPERTS LOOKING FOR MISSING ENRON E-MAIL [15 Jan 2002]

Lotus Notes e-mail messages ordered destroyed by a auditor whom Andersen has fired are now being searched by data-recovery experts using the same techniques used to look for suspected spy transmission and for Clinton White House correspondence sent by e-mail. A representative of Ontrack Data International says, "The general practitioner doesn't know that once you hit delete and get it out of your inbox that it's not gone. That is why this is a very fertile area for key evidence in litigation." Agencies such as the NSA, CIA and FBI go one extra step to keep deleted material from being recovered; they accomplish this through the use of software that repeatedly overwrites free space on hard drives. (AP/San Jose Mercury News 16 Jan 2002)

http://www.siliconvalley.com/docs/news/svfront/085710.htm

Category 13.2 Data corruption & destruction

2002-03-11 quality assurance QA design data integrity user interface documentation

RISKS 21 94ff

A couple of correspondents wrote in to RISKS with yet another litany of complaints about Microsoft Office products that change input data unexpectedly. Both found that grades they were entering were being modified; one found that incorrect spellings were being forced, including into e-mail addresses. One complained about mysterious lines and bullets appearing in his text.

[MK comments: Everything the correspondents described is controlled through options available through the Tools menu item in Office products. Both correspondents illustrate the dangers resulting from the combination of bloatware (programs with enormous lists of functions and features) coupled with poor user interface design and inadequate training. Office products typically do not provide a visual indicator of the status of various "helpful" features such as the "AutoCorrect" and "Enable Autocomplete for Cell Values" functions. A user unaware of the existence of these functions has no clue where to look for the mysterious source of inexplicable data transformations, let alone any idea of how to turn them off.

MORAL: system administrators should set all autocorrection and autoformatting features OFF by default when delivering systems to novice users and should provide training to allow controlled reactivation of those features that the users feel will be helpful and controllable.]

Category 13.2 Data corruption & destruction

2002-03-12 speech recognition default documentation data integrity corruption feature

awareness

RISKS 21 95

Hawkins Dale reported on another case of data corruption by default in RISKS:

>Slashdot (slashdot.org) and others are reporting that "some Windows XP users are finding random words inserted into their text as they write. The problem is caused by XP's speech recognition system, which is turned on by default by some manufacturers. It's listening to the random noise you get even when the mic is turned off."

Microsoft is blaming the problem on some computer manufacturers who enable this feature by default in their installation of the operating system.

Draw your own conclusions regarding the risks of adding powerful features that users are unaware of.<

Category 13.2 Data corruption & destruction

2002-03-19 archives dynamic content technology change

NewsScan

#### FOR LONG-TERM DOCUMENT PRESERVATION, YOU NEED TO EMULATE

RAND Corporation researcher Jeff Rothenberg says that for long-term document preservation you need to use emulation. "If you think about anything in digital form, the article itself is a program. Not the way we usually think about it, but even a string of ASCII codes is a program, a sequence of little commands, each of which is interpreted by some simple interpreter that knows how to draw those characters on the screen and knows how to do what the command says. If you don't have the right interpreter, the one that knows what each of these commands means, then you don't have the document. You might have some aspect of it, but you've lost the original's behavior. And just looking at Web pages, fewer sites consist of static HTML. There's lots of stuff that gets generated on the fly, Javascript, server-side Java, Active Server pages. If all you save is the text of those pages, you haven't got it, and that kind of convinces me that digital documents must be executable in the future to really preserve them." (IEEE Software Mar/Apr 2002)

http://computer.org/software/so2002/s2toc.htm/(sub req'd)

Category 13.2 Data corruption & destruction

2002-05-22 backup disk failure data loss law enforcement police

RISKS 22 08

Thomas Insel wrote in RISKS:

On 11 May 2002, \*The New York Times\* (page A13 of the National Edition) reported that the Macomb County, Michigan, sheriff's department lost over 50,000 photographs of criminals on a crashed hard drive. Not particularly exciting, except that they had wisely made hardcopy backups of some of the photos. The issue of electronic backups was never even raised. Perhaps many computer users no longer realize such a thing is possible? http://www.nytimes.com/2002/05/11/national/11BRFS.html

Category 13.2 Data corruption & destruction

2002-07-22 wrong number incorrect data QA quality assurance lawsuit penalties payment costs

NewsScan

#### WRONG NUMBER COSTS GATEWAY \$3.6 MILLION

A federal court has awarded a Pensacola business \$3.6 million in damages from Gateway, which had accidentally distributed the wrong phone number for customer complaints to more than 275 Gateway stores. The error dated back to 1999, when someone at Gateway erred by using the 800 prefix instead of the correct 888 prefix for the company's toll-free customer complaint line. The wrong number was also posted on Gateway's Web site, listed on Internet billings and included on a form distributed to more than 100,000 Gateway customers. Mo' Money, which manufactures and distributes promotional items, said it contacted Gateway six days after the calls began, but that it took the computer company more than two years to fix the problem. "It was a nightmare," says Mo' Money president Cliff Mowe. "We had as many as 8,000 extra calls a month, and these were all angry people You couldn't get them off the line because the only number they had was ours. You'd have to explain it and go through it, and a lot of times they'd call you right back anyway." (AP 19 Jul 2002)

Category 13.2 Data corruption & destruction

2002-07-26 e-mail archives storage policy removal destruction data loss

NewsScan

#### HOTMAIL CLEAN-UP POLICY ANGERS USERS

Microsoft's Hotmail system has instituted a new storage policy that limits the time span for saved mail to 30 days. After that, it's automatically deleted from a user's Sent file -- an action that has left many users steaming. Desperate users who've pleaded for their mail back have been told it's irretrievable, and company officials say they warned users in mid-June of the change in policy. MSN product manager Parul Shah said users could avoid the problem by creating special folders and moving important messages out of the Sent file. The company is hoping the change in policy will prompt people to sign up for a fee-based version of the service that costs \$19.95 a month for an additional 8MB of storage on top of the 2MB they get for free. Microsoft says it has more than 110 million Hotmail users, but that so far fewer than 300,000 have signed up for the extra storage feature. (CNet News.com 25 Jul 2002)

http://news.com.com/2100-1023-946430.html?tag=fd\_top

Category 13.2 Data corruption & destruction

2002-08-02 e-mail archives regulations securities industry regulations standards fines penalties

data destruction

#### NewsScan

#### WALL STREET BANKS DISCARDED E-MAIL MESSAGES PREMATURELY

Six prominent firms (Citigroup, Morgan Stanley, Merrill Lynch, Deutsche Bank, and U.S. Bancorp Piper jaffraye) may be fined for as much as \$10 million for not keeping e-mail messages sent both within and outside the companies for three years. The penalties would come from the SEC, NASD, and the New Stock Exchange. (New York Times 2 Aug 2002)

# 13.4 Obsolescence

Category 13.4 Obsolescence

2002-04-24 research URL stability bibliography links evanescence disappearance automated

verification education

NewsScan

#### RESEARCHERS FOCUS ON 'LINK ROT'

Two researchers at the University of Nebraska are focusing their attention on so-called "link rot" -- broken hyperlinks -- which are becoming an increasing concern for professors and teachers who assign reading and research activities using the Web. The two professors monitored 515 hyperlinks over a period of 20 months and found that at the end of the time, 18.8% of the links had disappeared -- over 11% of the .org links, 18.4% of the .edu links, and 42.5% of the .com links were no longer active at the end of the study. Broken links included resources from the Mayo Clinic, an encyclopedia of plant biology, links on steroid use and links to courses with relevant lecture notes. The study also found that a few of the links had redirected to porn sites, which could be a real concern for teachers of younger students. The two professors are now working on a grant proposal to the National Science Foundation to develop software that would automatically check links for faculty and alert them by e-mail if the URL or content changes. (Wired.com 24 Apr 2002) http://www.wired.com/news/school/0,1383,51700,00.html

Category 13.4 Obsolescence

2002-08-30 archives obsolescense virtual computer emulation

NewsScan

#### 'UNIVERSAL VIRTUAL COMPUTER' BATTLES OBSOLESCENCE

A researcher at IBM's Almaden Research Center has proposed a system he hopes will eliminate the problem of digital document obsolescence, which threatens to undermine archivists' efforts to retain digital material for future generations. Dr. Raymond Lorie has developed a prototype for a "universal virtual computer," which features architecture and language designed to be so logical and accessible that computer developers of the future will be able to write instructions to emulate it on their machines. The software written for the universal virtual computer extracts all the data stored in a file, but does not try to include all the bells and whistles associated with that file. "I don't need to recreate Acrobat Reader with all its buttons and colors," says Lorie. "That would be overkill." Instead, the program uses tags to include extra semantic information that will indicate what the file is and how to read it. These semantic tags might say, for instance, "There is text in this document and it is organized like this," he explains. John Steenbakkers, director of information technology for the Dutch national library, says the universal virtual computer concept works. "We have seen a proof of concept. If the universal virtual computer became a standard for digital archiving, it would be a major step forward," offering a controlled, one-time migration to a specific preservation format. Meanwhile, Jeff Rothenberg of the RAND Corporation says Lorie's idea of data extraction is limited. "I would prefer to store documents in their original forms and formats -- with all of the software that created them and is typically required to view them." Data extraction "will give you the contents -- or rather, what someone thought were the meaningful core contents -- in some future form. But it won't preserve the original." (New York Times 29 Aug 2002)

# Viruses, virus-hoaxes, Trojans (assembly level or macro: not ActiveX or Java)

Category 14 Viruses, virus-hoaxes, Trojans (assembly level or macro: not ActiveX or Jav

2002-03-10 worldwide virus worm infection data top ten infectors malware

Trend World Virus Tracking Center

The new Trend World Virus Tracking Center < http://wtc.trendmicro.com/wtc/ > shows the top ten viruses observed in the wild through "actual virus infections detected by HouseCall, our free on-line virus scanner for PCs, and by the Trend Virus Control System (TVCS), our central management solution for network administrators." Viewers can easily select geographical areas and time periods of the last 24 hours, 7 days, or 30 days as well as details of each virus or worm. For example, as of 10 March 2002, the top ten infectors worldwide in the previous 30 days were as follows (showing the number of infected computers logged in parentheses) and a brief description of some of the malware types from Trend Micro's links to its comprehensive Virus Encyclopedia:

PE\_NIMDA.A-O (233,321) [This is a fast-spreading Internet worm and file infector in pure and original form. It arrives as an embedded attachment, README.EXE file, in an email that has an empty message body and, usually, an empty subject field. It does not require the email receiver to open the attachment for it to execute. It uses a known vulnerability in Internet Explorer-based email clients to execute the file attachment automatically. This is also known as Automatic Execution of Embedded MIME type. The infected email contains the executable attachment registered as content-type of audio/x-wav so that when recipients view the infected email, the default application associated with audio files is opened. This is usually the Windows Media Player. The embedded EXE file cannot be viewed in Microsoft Outlook.]

WORM\_SIRCAM.A (113,409) [This Worm is a high-level program created in Delphi that propagates via email using SMTP commands. It sends copies of itself to all addresses listed in an infected user's address book and in temporary Internet cached files. It arrives with a random subject line, and an attachment by the same name. This Worm also propagates via shared network drives.]

PE\_NIMDA.A (74,724) [

PE\_MAGISTR.B (64,199) [This variant of PE\_MAGISTR.A has polymorphic capabilities. It obtains email addresses from \*.WAB, \*.DBX, and \*.MBX files found in the infected system's disk and then sends emails with its infected files as attachments. It may also include non-viral files such as .DOC, .GIF, and .TXT files as attachments to the emails it sends out.This destructive variant trashes the Hard Drive and deletes certain files.]

PE\_FUNLOVE.4099 (56,146) [This virus infects all Win32 type Portable Executable (PE) files such as .EXE, .SCR, and .OCX in both Windows 9x and Windows NT 4.0. platforms. It searches for all Shared Network Folders with write access and then infects the files within them. To infect NT system files, the virus patches the integrity checking.]

PE\_NIMDA.E (46,722)

PE\_MAGISTR.A (37,346)

WORM\_BADTRANS.B (36,157) [This memory-resident Internet worm is a variant of WORM\_BADTRANS.A. It propagates via MAPI32, has a Key Logger component, and arrives with randomly selected double-extension filenames. It does not require the email receiver to open the attachment for it to execute. It uses a known vulnerability in Internet Explorer-based email clients (Microsoft Outlook and Microsoft Outlook Express) to automatically execute the file attachment. This is also known as Automatic Execution of Embedded MIME type.]

JS\_EXCEPTION.GEN (31,733) [This Java Script (JS) Trojan changes the infected user's Internet Explorer startup page. One of this Trojan's samples (Coolsite samples) is a mass-mailer. It exploits security vulnerabilities in the Microsoft Virtual Machine. Some variants have non-destructive payloads that change the button caption, modify the appearance of Internet Explorer, and redirect links to a certain Web site.]

WORM.KLEZ.E (28,057) [This destructive mass-mailing worm propagates copies of itself across network drives. Upon execution, it drops two executable files, WINK\*.EXE and WQK.EXE, in the Windows System folder. It also creates registry entries that allow it to run at system startup.

This worm terminates processes, and occasionally deletes files associated with certain antivirus programs. On the sixth (6) day of every odd-numbered month (January, March, May, July, September, November) it overwrites files with the following extensions: TXT, HTM, HTML, WAB, DOC, XLS, CPP, C, PAS, MPEG, MPG, BAK, MP3, JPG.]

# 14.1 Viruses

Category 14.1 Viruses

2002-01-10 macro virus .NET proof-of-concept demonstration

NewsScan

#### NEW "PROOF-OF-CONCEPT" VIRUS [10 Jan 2002]

A Czech programmer has created a "proof-of-concept" virus called W32/Donut to alert security antivirus vendors and Microsoft managers of software vulnerabilities in executable files created for Microsoft's .NET Web services technology. A spokesman for Symantec, a major vendor of security software, says that the virus "does not have any significant chance to become widespread. However, it shows that virus writers are paying close attention to the new .NET architecture from Microsoft and are attempting to understand the framework that eventually will be available on most systems." (Reuters/USA Today 10 Jan 2002)

http://www.usatoday.com/life/cyber/tech/2002/01/10/microsoft-dot-net-virus.h tm

Category 14.1 Viruses

2002-03-27 worm picture cartoon e-mail social engineering Trojan

NewsScan

#### CLINTON CARTOON CARRIES VIRUS

McAfee, the anti-virus software company, says a new virus called MyLife.B., is being circulated as an e-mail attachment featuring a cartoon about former president Bill Clinton. A McAfee executive says, "If this one does reach large proportions, it will be a very costly virus because most consumers don't have good backup methods for their operating system or important files on the C drive." The virus e-mails itself to everyone in a user's Microsoft Outlook address book or MSN Messenger contact list. The virus will cause damage only if you open the attachment - so don't open it! (USA Today 26 Mar 2002) http://www.usatoday.com/life/cyber/tech/2002/03/26/viruses.htm

Category 14.1 Viruses

2002-04-22 virus proof-of-concept programming language Vx virus exchange

Security Wire Digest 4 31

#### \*FIRST SAP VIRUS, NO WORRIES

Virus writers targeted another exotic programming language last week, but McAfee.com and Symantec report that the proof-of-concept ABAP.Rivpas.A virus doesn't work. It was written in the Advanced Business Application Programming language used by many large corporations to infect programs and reports used by the SAP R/3 business information system. The "intended virus" was first posted to a virus exchange Web site last year.

http://vil.nai.com/vil/content/v\_99453.htm

Category 14.1 Viruses

2002-06-14 malware virus picture proof-of-concept jpg steganography

NewsScan

#### NEW VIRUS CAN INFECT PICTURE FILES

McAfee Security is reporting that a new virus called "Perrun" is the first ever to infect picture files, which, along with other data files, have long been considered safe from such threats. Researchers at McAfee received the virus from its creator and say it's what's called a proof-of-concept virus and does not cause any damage. Up until now, viruses infected and were spread through program files; data files might be deleted or damaged, but Perrun is the first to infect them by inserting portions of the virus code into the picture file. When a JPG picture is viewed, the virus installs a file on the victim's hard drive that can infect other pictures. Because the original picture looks fine, the victim won't know that anything's amiss. (AP 13 Jun 2002) http://apnews.excite.com/article/20020613/D7K4F4EG1.html

Category 14.1 Viruses

2002-08-13 virus malware worm incidence growth

NewsScan

#### ALL QUIET ON THE VIRUS FRONT

It's been a slow year for computer virus experts, with the Klez e-mail worm the only notable annoyance now making the rounds. "Klez is the biggest case of the year and that's it," says Mikko Hypponen, manager of antivirus research at Finland's F-Secure. "That's a big surprise to us and to everybody else in the antivirus community." Other monitoring firms report similar findings: Sophos Anti-Virus in the UK says it's detecting 600 to 700 new virus types per month -- about half as many as last year. Theories on why 2002 has seen a significant drop in viruses vary, ranging from the introduction of enhanced antivirus software to stiffer anti-hacker laws to more vigilant computer users. "For the antivirus industry in general, a slow-down would not be very good," says Hypponen. "But I'd love to see it happen. It would free up the resources for us to do something other than fight a problem that shouldn't even be there in the first place." (Reuters 13 Aug 2002)

Category 14.1 Viruses

2002-09-20 virus writer arrest Linux operating system

NewsScan

ARRESTS: . . . . VIRUS CREATION

In London, law enforcement officials at Scotland Yard have arrested a 21-year-old programmer they say created the T0rn (with a zero) virus, which was designed to do malicious damage to Linux computer systems.... (Reuters and New York Times 19 Sep 2002)

# 14.2 Worms

Category 14.2 Worms

2002-05-05 worm virus e-mail social engineering

RISKS 22 05ff

By early May 2002, the KLEZ.H worm/virus was spreading extremely fast on the Internet and was having secondary effects. For one thing, because of the habit of forging e-mail headers to make it look as if someone on a victim's address list was the originator, many non-infected people were receiving angry e-mail from victims claiming that they were spawning infected e-mail. Worse, some of the recipients complained to system administrators or ISPs, causing much confusion and wasted effort as everyone had to figure out that the supposed originator was nothing of the sort. For another, some of the anti-virus products were firing off automated warnings to the supposed originators of infected messages; when these recipients happened to have enabled autoreply messages (the dreaded "I am out of the office" script), there was a real risk of mailstorms as each additional message from the supposedly infected source prompted yet another warning. Bounce messages also contributed to the mayhem.

Category 14.2 Worms

2002-05-05 worm virus e-mail social engineering

RISKS 22 05

In April 2002, a variant of the the KLEZ worm family known since November 2001 became a major threat to MS Outlook users worldwide. Peter G. Neumann summarized the situation:

A rogue computer program that is the online equivalent of a quick-change artist is infecting computers around the world via email and clogging computer networks. The program, W32/KLEZ.H, is a "blended threat," combining elements of a virus, which infects machines, and a worm, which transports itself from machine to machine. It also tries to disable some antivirus programs. It makes itself hard for users to spot by changing its e-mail subject line, message and name of the attachment at random, drawing from a database that includes, for example, such subject lines as "Hello, honey," and "A very funny Web site." The program has grown increasingly common as users unknowingly activate it sometimes without even opening the e-mail attachment that carries the virus and allow it to send copies of itself to those in the victim's e-mail address file.

Category 14.2 Worms

2002-05-20 worm vulnerability exploit browser

Security Wire Digest 4 39

#### \*NEW WORM ON THE PROWL

A new worm called W32.Yaha.c@mm is slowly making inroads on users' computers by capitalizing on unpatched Microsoft Windows systems. Exploiting the "Incorrect MIME Header Can Cause IE to Execute E-mail Attachment" vulnerability, it uses a two-part extension. The first is chosen from .doc, .mp3, .xls, .wav, .txt, .jpg, .gif, .dat, .bmp, .htm, .mpg, .mdb or .zip. The second is chosen from .pif, .bat or .scr. The worm searches an infected user's hard drive, address book and Instant Message programs for e-mail addresses and then mass mails itself. However, the worm is flawed and won't work unless MSN Messenger is installed on a system.

Category 14.2 Worms

2002-05-21 **P2P** peer-to-peer networks file sharing worm attack sabotage information warfare infowar motivation pornography

FindLaw Download This 86

#### ITS CREATOR SAYS KAZAA BENJAMIN WORM MEANS WELL

The creators of a new worm that targets users of the Kazaa file-trading network say they released the code to frustrate Internet users searching for pirated software and child pornography. Anti-virus software vendors have issued warnings that the so-called "Benjamin worm" is being unintentionally propagated among Kazaa users who download any of dozens of executable programs and screen savers that have been infected with the malicious code. According to one of its developers, Paul Komoszki, Benjamin is a "controlled test" of a program designed to disrupt the illegal exchange of copyrighted data and child porn over peer-to-peer networks.

http://www.newsbytes.com/news/02/176684.html

Category 14.2 Worms

2002-09-18 malware worm Linux servers denial-of-service attack DoS

NewsScan

#### 'SLAPPER' WORM IS A DRONE-IN-WAITING

The computer security firm Network Associates is calling attention to "Slapper," an invasive network "worm" capable of insinuating its way into Linux server computer systems and waiting until it, and many others like it, are activated to produce denial-of-service attacks that can overwhelm targeted Web sites. Network Associates' researcher Jimmy Kuo says the worm is being closely monitored and currently presents no great risk, but says "it could turn on a dime and become a wide spreader if someone fed in a new version." (Reuters/USA Today 2002)

Category 14.2 Worms

2002-10-01 worm back door keystroke logger bug flaw browser known vulnerability e-mail

NewsScan

#### ANOTHER WORM ATTACKS INTERNET EXPLORER: THE BUGBEAR

Taking advantage of a known vulnerability in Microsoft's Internet Explorer software, the Bugbear worm now moving around the world opens up a back door in the computers and logs keystrokes. But a bug in the worm (this is beginning to sound silly) has prevented Bugbear from taking over the address list on a computer and sending itself to new people. Ranked now as only a "medium risk" nuisance, it appears under a large variety of names but the attachment typically has a double file extension, such as .doc.pif. (Forbes 30 Sep 2002)

# 14.3 Virus/worms

Category 14.3 Virus/worms

2002-05-04 worm e-mail enabled virus Outlook address books flooding spam

NIPC Daily Report

On 4 May, an outbreak of the "W32.Magister" computer virus [worm] has apparently struck businesses in Europe, the U.S., and elsewhere. Businesses reported receiving dozens of unsolicited e-mail. Replies and requests to be removed from any mailing lists involved only resulted in a flood of additional e-mail. Companies in the Netherlands, France, New Zealand, the U.K. and the U.S. were similarly affected, including such large multinationals as Unilever and Diageo. Many of the recipients were businesses in the food industry that subscribed to an e-mail newsletter service from Foodnavigator.com. The culprit appears to be the W32.Magistr.24876@mm virus. The virus infects Windows Portable Executable files. It then gathers e-mail addresses from Outlook and Outlook Express mail folders, Windows address books, and the sent items file in Netscape, and sends out multiple e-mail messages. According to the Symantec Anti-virus Research Center, the virus was first discovered on 13 March, and there have been at least 50 confirmed infections affecting more than ten sites since then. (Source: Newsbytes, 5 May)

# 14.4 Trojans

Category 14.4 Trojans

2002-01-19 Trojan horse back door porn fraud scumware

RISKS 21 87

A patch for a vulnerability in the AOL Instant Messenger (AIM) program was converted into a Trojan horse that initiated unauthorized click-throughs on advertising icons, divulged system information to third parties and browsed to porn sites.

Category 14.4 Trojans

2002-03-11 Trojan horse executable attachment patch social engineering worm

RISKS 21 94

The "Gibe" worm was circulated in March 2002 as a 160KB EXE file attached to a cover message pretending to be a Microsoft alert explaining that the file was a "cumulative patch" and pointing vaguely to a Microsoft security site. Going to the site showed no sign of any such patch, nor was there a digital signature for the file. However, naive recipients were susceptible to the trick.

[MORAL: keep warning recipients not to open unsolicited attachments in e-mail.]

Category 14.4 Trojans

2002-04-03 P2P peer-to-peer Trojan distributed computing storage EULA end-user license

agreement

RISKS, http://news.com.com/2100-1023-873181.html

22 02

Nicholas C. Weaver warned in RISKS that the company Brilliant Digital (BD) formally announced distribution of Trojan software via the Kazaa peer-to-peer network software. The BD software would create a P2P server network to be used for distributed storage, computation and communication -- all of which would pose serious security risks to everyone concerned. Weaver pointed out that today's naïve users appear to be ready to agree to anything at all that is included in a license agreement, whether it is in their interests or not.

Category 14.4 Trojans

2002-05-20 Java Scrip Trojan HTML Web page e-mail data corruption integrity

Security Wire Digest 4 39

#### \*MALICIOUS PORN ADS STALK USERS

Antivirus experts say users no longer need to be concerned about JS.Fortnight, a Java Script Trojan that was embedded in a now-defunct Web page. Upon visiting that site, a user's Outlook Express signature would be modified to include a link back to the porn site in every message sent.

# 14.5 Virus hoaxes

Category 14.5 Virus hoaxes
2002-05-20 social engineering hoax meme virus warning file deletion

Security Wire Digest 4 39

The lastest social-engineering virus hoax of May 2002 involved detailed instructions on how to remove the "virus-infected" file JDBGMGR.EXE. Unfortunately, this harmful file is the Microsoft Debugger Registrar for Java and its removal causes some Java applets to fail. Apparently the hoax was circulating in English, French, Italian, Spanish, Dutch and German versions.

### **15.1** Fraud

Category 15.1 Fraud

2002-02-25 online fraud credit card charges debit checking lawsuit

NewsScan

#### AOL ACCUSED OF CHARGING FOR UNWANTED GOODS [25 Feb 2002]

America Online has been named in a lawsuit for allegedly charging thousands of customers for merchandise, such as books and stereos, that they did not order. The suit, which is seeking class-action status, claims that AOL "unlawfully charged and collected money for this unordered merchandise and shipping and handling charges from credit card, debit card and checking accounts." The plaintiffs are seeking unspecified damages, the refund of unauthorized payments, and the consumers' retention of the unauthorized merchandise at AOL's expense. Meanwhile, an AOL spokesman said the "allegations are without merit and we intend to vigorously contest this lawsuit in court." (AP 25 Feb 2002) http://apnews.excite.com/article/20020226/D7HTDUH80.html

Category 15.1 Fraud

2002-02-26 lawsuit fraud online merchandise orders charges credit card

NewsScan; http://apnews.excite.com/article/20020226/D7HTDUH80.html

#### AOL ACCUSED OF CHARGING FOR UNWANTED GOODS

America Online has been named in a lawsuit for allegedly charging thousands of customers for merchandise, such as books and stereos, that they did not order. The suit, which is seeking class-action status, claims that AOL "unlawfully charged and collected money for this unordered merchandise and shipping and handling charges from credit card, debit card and checking accounts." The plaintiffs are seeking unspecified damages, the refund of unauthorized payments, and the consumers' retention of the unauthorized merchandise at AOL's expense. Meanwhile, an AOL spokesman said the "allegations are without merit and we intend to vigorously contest this lawsuit in court." (AP 25 Feb 2002)

Category 15.1 Fraud

2002-04-15 fraud scam speculation foreign currency arbitrage consumer loss

NewsScan; http://www.siliconvalley.com/mld/siliconvalley/3067032.htm

#### BETTING MONEY ON MONEY

Speculation on foreign currencies is now a sport -- a dangerous one -- that can be played by small players who use Web sites to access the world's 24-hour currency markets. But financial experts advise investors to stick to blackjack or some slower way to lose their money. Harvard economist Dani Rodrik says, "I certainly wouldn't advise this for my mother-in-law. This is an area where it's much harder for an individual investor have a good nose for, than stocks or bonds." Unlike stock-trading, currency speculation is a zero-sum game (when you win, your opponents lose, and your opponents are mega-institutions such as Deutsche Bank, who know the game better that you ever will). There are also scam artists to watch out for, and in the past two years the U.S. Commodity Futures Trading Commission put a stop to schemes that had scammed 1,000 traders out of more than \$60 million. (AP/San Jose Mercury News 14 Apr 2002)

Category 15.1 Fraud

2002-04-16 Internet fraud complaints statistics 4-1-9 Nigerian online auctions

NewsScan

#### INTERNET FRAUD

The Internet Fraud Complaint Center <a href="http://www.ifccfbi.gov">http://www.ifccfbi.gov</a>, a partnership between the FBI and the National White Collar Crime Center, says that almost 50,000 complaints were filed last year on its site. About 2 out of 5 were related to online auctions, and 1 out of 6 involved the "Nigerian Letter Fraud," where the recipient of an Internet message gets a phony offer to make a big commission for helping the message sender transfer millions of dollars illegally out of Nigeria. (New York Times 15 Apr 2002)

http://www.nytimes.com/2002/04/15/technology/15SCAM.html

Category 15.1 Fraud

2002-05-21 Internet pharmacy prescription prosecution international

FindLaw Download This 86

#### CHARGES AGAINST INTERNET PHARMACY

In recent years, busloads of Americans have crossed into Canada to buy cheaper prescription drugs with help from Canadian doctors. Now many of those customers, mostly senior citizens facing large medicine bills, make that trip by the Internet, creating a growing industry that is attracting the attention of regulators. On May 14, the Ontario College of Pharmacists filed the province's first charges against a Web site selling prescription drugs, accusing it of doing so without a license. It is the initial salvo in what could be a lengthy battle over how to regulate the Internet prescription drug industry, raising questions about whether technology has advanced faster than the governing laws and policies.

http://news.findlaw.com/ap/ht/1700/5-19-2002/20020519130003\_03.html

Explore FindLaw's Health Law Resources http://www.findlaw.com/01topics/19health/index.html

Category 15.1 Fraud

2002-05-23 4-1-9 Nigerian scam variant

NewsScan

#### PHONY 'SOLDIER' NEEDS YOUR HELP GIVING HIM YOUR MONEY

A scam e-mail message now circulating the Internet purports to be from a "Special Forces Commando" in Afghanistan who's found \$36 million in drug money while on patrol, and who wants your help in moving the cash. Sure he does. "We will thus send you the shipment waybill, so that you can help claim this luggage on behalf of me and my colleagues. Needless to say the trust in you at this juncture is enormous. We are willing to offer you an agreeable percentage of funds." Stop laughing, and grab onto your wallet. (AP/San Jose Mercury News 23 May 2002) http://www.siliconvalley.com/mld/siliconvalley/3319360.htm

Category 15.1 Fraud

2002-05-28 fraud scam URL DNS domain name system misspellings pornography theft investigation pursuit mouse-trapping HTML

FindLaw Download This; http://news.findlaw.com/ap/ht/1700/5-24-2002/20020524120012\_14.html

#### INTERNET SCAM ARTIST FINED \$1.9M

In May 2002, John Zuccarini of Andalusia, Pa., was ordered to pay \$1.9 million in restitution to victims of his URL-misspelling scam, in which he registered more than 5,500 Web sites with names similar to celebrities and popular organizations such as the Backstreet Boys, Bank of America, Victoria's Secret, and The Wall Street Journal. In particular, Zuccarini registered 15 variations on the name of the Cartoon Network site and 41 versions of Britney Spears' name. The scam worked by forcing accidental visitors into click-through advertisements and disabling their ability to leave the site; sometimes the back and close buttons were inoperative. Another deceptive technique involved a "stealth page" concealed under the task bar, usually at the bottom of the screen. This window activated a timer that popped up yet more ad windows at the beleaguered viewer. Money came from advertisers who were also being cheated, since most of the clickthroughs were in fact from unwilling victims of the scam. By October 2001, Zuccarini had already been sued by 63 groups in the two years and lost 53 times. He had been subjected to 56 arbitration proceedings and lost rights to about 200 of his misspelled domains, yet he continued to rack up profits using his schemes. The US Federal Trade Commission (FTC) filed a complaint against Zuccarini, "doing business as The Country Walk, JZDesign, RaveClub Berlin, and more than 22 names incorporating the word "Cupcake," including Cupcake Party, Cupcake-Party, Cupcake Parties, Cupcake Patrol, Cupcake Incident, and Cupcake Messenger." Unfortunately, Zuccarini remained at large despite attempts of law enforcement officials to locate him.

87

Category 15.1 Fraud

2002-06-06 fraud hacking contest penetration criminal hackers

Security Wire Digest 4 44

#### \*HACKING CONTEST CHALLENGED

A Korean hacking contest is under fire for skimping on the prize money, exposing private data on contestants and maybe conning them with a false server running few activated services. When hackers "kill9" and "m0rla posted" discovered that the contest target network was an Apache server running few services on a non-standard port, they decided to break into the contest sponsor's host, Korea Digital Works (KDW). Among the duo's findings were personal data on the 1,240 contestants-319 of them from the United States. The event, sponsored by several Korean IT organizations, had promised \$100,000 to the first contestant to hack into the decoy server or five \$10,000 to those who made the best attempts. One winner, however, claims he's only been offered \$1,250 and must provide bank details to collect it. That's made contestant Bill Wong of New York wonder if the message from KDW or the contest itself was an elaborate hoax. KDW earlier said contestants from 51 countries participated in the challenge and argues it hasn't mishandled the competition.

Category 15.1 Fraud

2002-07-15 fraud education consumer warnings search engine

NewsScan

#### FTC 'TEASER' SITES TAKE AIM AT UNWARY CONSUMERS

The Federal Trade Commission and the Securities and Exchange Commission have teamed up to create some number of "teaser" sites that pop up among the results on search engines when users type in requests for everything from "free vacations" to "erectile dysfunction cures." The teaser sites open with a page featuring "too-good-to-be-true" offers, and then when the unsuspecting user clicks for details, the screen switches to a young man holding out his hand to say "Stop!" with the headline "You could get scammed!". FTC attorney Eric Wenger says the ads represent the agency's attempt to reach consumers before they are victims of fraud. "We want to try to reach out to them and give them information that they can use to critically evaluate offers that they are receiving. And allow them to recognize and avoid deception before falling victim to it." He says the sites are designed to educate and empower consumers, not to make them feel silly or like they've been "had." The sites also provide links to complaint forms and tips provided by the FTC at www.ftc.gov. (CNN.com 11 Jul 2002)

Category 15.1 Fraud

2002-12-06 e-commerce Web advertising links pop-up banner ads alerts class-action lawsuit deception deceptive business practices

NewsScan

#### LAWSUIT CHALLENGES DECEPTIVE AD-LINKS

A class action lawsuit has been filed against Internet portal Bonzi.com, accusing the company of tricking users into visiting its Web site by creating pop-up banner ads disguised as system alerts or security alerts, and directing people who click on the alert messages to the Bonzi site and its ads for software and other products. San Francisco lawyer Evan Cox, who specializes in Internet law, doubts the plaintiffs will be successful: "The approach is interesting, and there my be a lot of people out there rooting for the plaintiff on an emotional level, but the complaint is probably an uphill battle on most of its courses of action." Of course, the lawyers who filed the suit are more optimistic; one of them, Darrell Scott, says: "The Internet has unfortunately become a cornucopia for deceptive business practices. Class-based civil litigation will hopefully establish that the Internet is not, as some think, a sanctuary for those who engage in deception." (InfoWorld 5 Dec 2002) http://www.infoworld.com/articles/hn/xml/02/12/05/021205hnsuit.xml?s=IDGNS

# 15.2 Extortion

Category 15.2 Extortion

2002-06-18 DNS Domain Name System governance control confidentiality sequestration

password cryptographic key

FindLaw Download This

#### CULT HERO HOLDS DOMAIN HOSTAGE

The administrator of South Africa's web addresses said on Thursday he had hidden the key to the country's ".ZA" domain network abroad to prevent any government interference in access to the Internet. South Africa's parliament has given initial approval to a law that will allow the government to take control of the country's Internet address administration. But critics, including ZA domain-name administrator Mike Lawrie, say the government has no right to stage the takeover and warn it could collapse the domestic Internet structure.

http://zdnet.com.com/2100-1105-935968.html

South African Legal Resources

http://www.findlaw.com/12international/countries/za.html

# 16.1 Industrial espionage

Category 16.1 Industrial espionage

2002-04-12 industrial espionage information warfare infowar international

NewsScan

#### ADDED INDICTMENTS IN STOLEN TRADE SECRETS CASE

Three Chinese citizens, two of whom were Lucent scientists in that company's Murray Hill, N.J., headquarters have been charged with stealing secrets from four companies in addition to Lucent. They had already been indicted for stealing secrets from Lucent, but are now being charged with similar crimes against Telenetworks, NetPlane Systems, Hughes Software Systems, and Ziatech. The three New Jersey residents -- Hai Lin, Kai Xu, and Yong-Qing Cheng, all in their 30s -- are thought to have developed a joint venture with the Datang Telecom Technology Company of Beijing to sell a clone of Lucent's Path Star data and voice transmission system to Internet providers in China. (AP/New York Times 12 Apr 2002) http://www.nytimes.com/2002/04/12/technology/12LUCE.html

Category 16.1 Industrial espionage

2002-09-20 criminal hacker arrest software theft intellectual property industrial espionage

infowar information warfare

#### NewsScan

#### ARRESTS: SOFTWARE THEFT....

.... In California's Silicon Valley, the FBI has arrested a Chinese programmer accused of trying to steal a software package used for seismic imaging of oil fields. The software was created by 3DGeo Development software company in Mountain View, California. The 32-year-old programmer, who is now in custody at the Santa Clara jail, has been in the U.S. since April as part of a contract between 3DGeo and his employer in China, the state-owned China National Petroleum Corporation. (Reuters and New York Times 19 Sep 2002)

# 16.2 Industrial information systems sabotage

Category 16.2

Industrial information systems sabotage

2002-06-26

proposed legislation law statute copyright violation retaliation revenge denial-ofservice attacks DOS peer-to-peer spoofing interception interdiction redirection cyberwar

#### NewsScan

#### LEGISLATION WOULD SANCTION STUDIO HACK ATTACKS

Proposed legislation crafted by California congressman Howard Berman, whose district includes Hollywood, would provide a shield against legal liability for copyright owners, such as record labels and movie studios, that used high-tech attacks against peer-to-peer Web sites to stop them from enabling illegal file-sharing. "While P2P technology is free to innovate new and more efficient methods of distribution that further exacerbate the piracy problem, copyright owners are not equally free to craft technological responses," says Berman. "This is not fair." Included in the actions a copyright holder would be allowed to take are: interdiction, in which the copyright holder swamps a P2P file server with false requests so that downloads can't get through; redirection, in which would-be file swappers are pointed to a site that doesn't contain the files they're seeking; and spoofing, in which a corrupt or otherwise undesirable file masquerades as the song or movie file being sought by a file swapper. File-swapping companies criticized the bill, saying it opens the door for copyright holders to conduct "cyber warfare" against consumers. (CNet News.com 25 Jun 2002)

http://news.com.com/2100-1023-939333.html?tag=fd\_top

# 16.3 Infrastructure protection

Category 16.3 Infrastructure protection

2002-01-17 critical infrastructure protection terrorism

NewsScan

#### FBI WARNS OF TERRORIST ATTACKS ON GOVERNMENT INFOSYSTEMS [17 Jan 2002]

The FBI's infrastructure-protection team has alerted law-enforcement officers and high-tech companies of the possibility of new terrorist attacks on or through utility, municipal, or state information systems. The warning was not specific with regard to time frame or geographic area and its urgency-level was not as high as previous general alerts issued by the government to all Americans. (AP/USA Today 17 Jan 2002)

http://www.usatoday.com/life/cyber/tech/2002/01/17/net-warning.htm

Category 16.3 Infrastructure protection

2002-01-24 data leakage Web infrastructure protection national security

Security Wire Digest 4 6

A National Infrastructure Protection Center (NIPC) Advisory recommended that Web sites be edited to remove sensitve data that could be useful to terrorists and other enemies of the US.

Category 16.3 Infrastructure protection

2002-01-25 homeland security airport scanners X-ray radiation privacy

NewsScan

#### I-SEE-YOU: AIRPORT SECURITY MACHINES PEEK THROUGH CLOTHING

New security devices being tested at the Orlando airport are designed to find explosives residue, hazardous materials, metal items, and are able to see through clothes; airlines whose passengers will be asked to volunteer for scanning include Delta, Virgin Atlantic, Swissair and British Airways. The body scanner is expected to be the most controversial of the five machines being tested, because it subjects a passenger to low-level X-rays that penetrate clothing. (AP/USA Today 25 Jan 2002) http://www.usatoday.com/life/cyber/tech/2002/01/25/airport-security.htm

Category 16.3 Infrastructure protection

2002-01-31 critical infrastructure protection law enforcement terrorists targets Web Internet

research

NewsScan

#### FBI SAYS TERRORISTS HAVE USED INTERNET TO FIND NEW TARGETS

The National Infrastructure Protection Center (NIPC), which is the FBI's top cyber-security unit, says that al-Qaeda terrorists were apparently using the Internet to seek targets among American dams and water-supply systems and to acquire information about certain insecticides and pest-control products. Information obtained by the NIPC indicates that the terrorists had sought information on the supervisory control and data acquisition networks that control water supplies and wastewater facilities. (AP/USA Today 31 Jan 2002)

http://www.usatoday.com/news/attack/2002/01/31/terrorists-net.htm

Category 16.3 Infrastructure protection

2002-03-06 international terrorism information warfare Web communication

NewsScan

#### NEW AL QAEDA ACTIVITY ON THE INTERNET

U.S. government officials say they've discovered the existence of new Web sites created by Al Qaeda. The terrorist organization has always relied heavily on the Internet for communicating among its worldwide members, and its use of public Internet cafes and kiosks has made its communications difficult to track. The group has members in as many as 60 different countries. (New York Times 6 Feb 2002)

http://partners.nytimes.com/2002/03/06/international/asia/06INQU.html

Category 16.3 Infrastructure protection

2002-03-08 information warfare infrastructure military communications financial systems attack

subversion interference

NewsScan; http://www.usatoday.com/life/cyber/tech/2002/03/07/cuba-cyberattack.htm

#### STUDYING CUBA'S ABILITY USE NET TO DISRUPT U.S.

A senior U.S. government official says that the Bush administration has begun a review of Cuba's ability to use the Internet to disrupt this country's military communications or damage other U.S. interests. Last month, White House technical advisor Richard Clarke told a congressional subcommittee that if the U.S. is attacked through cyberspace, it could respond militarily: "We reserve the right to respond in any way appropriate: through covert action, through military action, and any of the tools available to the president." (AP/USA Today 7 Mar 2002)

Category 16.3 Infrastructure protection

2002-03-13 emergency wireless communications network homeland defense infrastructure

cyberterrorism

#### NewsScan

#### CEOs PLANS NETWORK TO RESPOND TO TERRORIST ATTACK

A task force formed by the Business Roundtable, an organization of corporate chief executives, is planning a nationwide system called CEO Link, designed to allow corporations to communicate with each other in the event of a terrorist attack. The president of Business Roundtable said that the more than 40 top executives who worked on the project "are really looking to make a difference for the country. They aren't coming to the table with business agendas. They're looking at how to make the country more secure." The group is chaired by C. Michael Armstrong of AT&T, which is preparing the design of CEO Link at its own expense. The system will include a wireless phone network as well as a secure Web site. (Washington Post 13 Mar 2002)

http://washingtonpost.com/wp-dyn/articles/A16827-2002Mar12.html

Category 16.3 Infrastructure protection

2002-03-24 information warfare infowar cyberterrorism book review

RISKS 21 98

Noted infowar gadfly Winn Schwartau -- the cyberterrorism prophet everyone either loves or hates -- published another novel in 2002, \_Pearl Harbor Dot Com\_. Peter G. Neumann's review in RISKS read in part, "[T]his book seems to make a rather compelling novel out of a surprisingly large number of security and reliability risk threats that we have discussed here over the years. The story echoes one of the fundamental problems confronting Cassandra-like risks-avoidance protagonists and agonists alike, namely, that, because we have not yet had the electronic Pearl Harbor, people in power perceive that there is little need to fix the infrastructural problems, so why bother to listen to the doom-sayers who hype up the risks? Well, in this novel, one man's massive craving for vengeance reaches major proportions, and significant effects result on critical infrastructures. In the end, the good hackers contribute notably to the outcome.

The book is somewhere within the genre of technothrillers, with a typical mix of murder, mayhem, intrigue, computer-communication surveillance, and non-explicit s\*x. I enjoyed it. It is entertaining, and the convoluted plot is quite consistent, fairly tight, and to RISKS readers, each incident is technologically quite plausible -- because many of the attacks seem almost reminiscent of past RISKS cases, sometimes just scaled up a little."

Category 16.3 Infrastructure protection

2002-04-03 financial services database data mining investigation forensics terrorists

NewsScan; http://www.siliconvalley.com/mld/siliconvalley/2989812.htm

#### CAN BUSINESS DATABASES BE USED IN ANTI-TERRORIST WAR?

A group of major companies that includes American Express, Visa, JP Morgan, Fidelity Investments, and CapitalOne is studying corporate databases to determine whether they can be used to find terrorists. Such databases usually include information about a person's home and car ownership, occupation, magazine subscriptions, and so forth. A lawyer working for the group says, "We have to think about how to use information to create profiles about what a bad guy might look like. This is business folks coming together to talk about how we might think about these issues. If companies go off and do advocacy based on what they learn here, that's how business works." Privacy advocates are wary, and James X. Dempsey of the Center for Democracy and Technology says he hopes the use of corporate databases to find terrorists is not an idea that is being "oversold, or overbought." (AP/San Jose Mercury News 3 Apr 2003)

Category 16.3 Infrastructure protection

2002-04-17 globalization information warfare inforwar international vulnerability

NewsScan

#### ONE-FOURTH MELLON FINANCIAL'S I.T. WORK MOVED TO INDIA

The latest financial giant to move much of its information technology work outside U.S. borders, Mellon Financial will soon be sending a quarter of its routine software maintenance chores to India. (A study by the Meta Group consulting firm indicates that an Indian programmer can be hired for one-fourteenth the rate of an American programmer.) Mellon executive Ken Herz says the company hopes to have new work for all U.S. workers affected by the company's decision, and explains: "This project emphasizes our intent to focus Mellon technology talent on growth-related projects and have routine maintenance work done offshore." (San Jose Mercury News 16 Apr 2002)

http://www.siliconvalley.com/mld/siliconvalley/3077722.htm

Category 16.3 Infrastructure protection

2002-04-22 homeland security infrastructure protection government network GovNet

Security Wire Digest 4 31

#### \*CLARKE: GOVNET READY FOR NEXT PHASE

Despite no money earmarked for an actual program or project, U.S. cybersecurity czar Richard Clarke told a conference audience GovNet is moving forward. An impenetrable information network exclusively for the federal government is feasible, according to a General Services Administration review based on surveys from 167 technology companies. Clarke told federal IT workers last week that it's time to determine how much it will cost to build a tamper-proof network. Possible "paths" for GovNet include improving security on existing federal networks, allowing agencies to build their own stand-alone or multiagency networks, or utilize existing stand-alone networks and create a backup network in case there's a disaster or attack.

Category 16.3 Infrastructure protection

2002-05-07 information warfare infrastructure protection failure problems weakness vulnerability financial systems health data communications emergency

NewsScan; http://www.usatoday.com/life/cyber/tech/2002/05/06/cyber-terror.htm

#### UNPREPARED FOR CYBERATTACKS?

People with knowledge of national intelligence briefings say that little has been done to protect the country against a cyberattack. Senator Jon Kyl (R-Ariz.) says: "It's a big threat, because it is easy to do and can cause great harm," and vulnerable U.S. targets are said to include the Centers for Disease Control and Prevention; FedWire, the money-movement clearing system maintained by the Federal Reserve Board; computer systems that operate water-treatment plants or that run electrical grids and dams; facilities that control the flow of information over the Internet; the nation's communications network, including telephone and 911 call centers; and air traffic control, rail and public transportation systems. Rep. Jane Harman (D-Calif.) says: "What I fear is the combination of a cyberattack coordinated with more traditional terrorism, undermining our ability to respond to an attack when lives are in danger." (USA Today 6 May 2002)

Category 16.3 Infrastructure protection

2002-05-24 homeland security cybersecurity information warfare government budget funding research expenditures critical infrastructure

NewsScan

#### CYBERSECURITY GETS \$1.7 BILLION BOOST IN BUDGET

The Bush Administration has included a \$1.7 billion increase in cybersecurity in its proposed budget -- 68% over its current level. Last fall a congressional survey gave a grade of "F" to 17 of 24 major federal agencies for their level of security preparations. In the new budget, overall technology spending by the federal government will increase from \$45 billion to \$52 billion, but Department of Commerce undersecretary Ken Juster notes that 90% of the nation's critical infrastructure (e.g., transportation and communication systems and power grids) is privately owned and operated, and suggests: "The insurance and legal industries should reward companies" that make computer security "as integral a part of their business as marketing and product development." (The Record, Hackensack NJ/San Jose Mercury News 23 May 2002) http://www.siliconvalley.com/mld/siliconvalley/3324403.htm SECURITY

Category 16.3 Infrastructure protection

2002-06-27 infrastructure protection terrorism distribution control systems DCS supervisory

control data acquisition SCADA 911

#### NewsScan

#### OFFICIALS FEAR TERRORIST ATTACKS ON DCS AND SCADA SYSTEMS

For some months now the FBI has been evaluating evidence that al-Quaida terrorists located throughout the world have been trying to develop ways to use the Internet to interfere with the control of major physical systems in the U.S., such as dams, utility systems, nuclear power plants, and so forth. Those kinds of facilities are managed through digitally systems called "distributed-control systems" (DCS) and "supervisory control and data acquisition" (SCADA) systems. Systems like that were typically not designed with public access in mind, so they usually lack even rudimentary security protection. The director of the FBI's National Infrastructure Protection Center said last month: "The event I fear most is a physical attack in conjunction with a successful cyber-attack on the responders' 911 system or on the power grid." (Wash Post/San Jose Mercury-News 27 Jun 2002)

http://www.siliconvalley.com/mld/siliconvalley/3554402.htm

Category 16.3 Infrastructure protection

2002-06-27 security flaws obscurity national security quality assurance QA

RISKS 22 13

Brien Webb wrote an interesting analysis of Microsoft testimony:

>From a 2002/05/13 article by Caron Carlson in eweek.com:

http://www.eweek.com/article/0,3658,s%253D701%2526a%253D26875,00.asp

"A senior Microsoft Corp. executive [Jim Allchin] told a federal court last week that sharing information with competitors could damage national security and even threaten the U.S. war effort in Afghanistan. He later acknowledged that some Microsoft code was so flawed it could not be safely disclosed."

and later, directly quoting Allchin...

"Computers, including many running Windows operating systems, are used throughout the United States Department of Defense and by the armed forces of the United States in Afghanistan and elsewhere."

Microsoft proposes to withhold details of the MSMQ protocol (TCP port 1801 and UDP port 3527), the Windows File Protection API, as well as APIs for anti-piracy protection and digital rights management under the security carve-out.

I recall that the Windows NT family of operating systems was designed to meet DOD's C2 security criteria, including the Orange Book (standalone, which they passed), as well as Red Book (networking) and Blue Book (subsystems) criteria which they started working on at least 4 years ago; I don't know if they've yet passed, but I suspect not if it's so flawed that they don't want to disclose the protocol or API! See

http://msdn.microsoft.com/library/default.asp? url=/library/en- us/dnproasp2/html/windowsntsecuritysystems.asp

So, one risk of flawed software might be that you have to publicly invoke national security (read patriotism) as a last refuge from legal process.<

Category 16.3 Infrastructure protection

2002-07-25 cyberterrorism information warfare infrastructure protection homeland defense

NewsScan

#### THE RISKS FROM CYBERTERRORISM

Cybersecurity experts are busy lobbying Congress for protections from liability lawsuits but some analysts say the media may be over-stating the risks from terrorist cyber attacks. Marc Maiffret of eEye Digital Security says, "Terrorists are only recently starting to realize the benefits of having people within their organizations that have real hacking skills," and University of South California professor of communications Douglas Thomas adds: "Cyber-terrorism is a lot more difficult than many people assume." Even so, security expert Stanley Jarocki warns that terrorists could do a lot of damage by cracking U.S. corporate systems: "Today, some say it would be easier for a terrorist to attack a dam by hacking into its command-and-control computer network than it would be to obtain and deliver the tons of explosives needed to blow it up. Even more frightening, such destruction can be launched remotely, either from the safety of the terrorist's living room, or their hideout cave." (AP/USA Today 24 Jul 2002)

http://www.usatoday.com/tech/news/computersecurity/2002... protection\_x.htm

Category 16.3 Infrastructure protection

2002-08-22 wireless emergency response communications network law enforcement

government infrastructure protection

NewsScan

#### IBM TEAMS WITH U.S. GOV'T ON WIRELESS EMERGENCY NETWORK

IBM is working with a consortium of government agencies to build a wireless emergency network that will enable police, fire and safety groups in the Washington, DC area to communicate with each other in real time via instant messaging. The Capital Wireless Integrated Network (CapWIN) — the first such network in the nation — will run on top of existing communications and computer systems and will be accessible via standard PCs, handhelds and cell phones. "The purpose of CapWIN is to enable these functions by leveraging existing networks and systems... The hard part is going to be to make sure that we get the user requirements defined correctly the first time," says Kent Blossom, director of safety and security systems for IBM, which will supply clustered eServers to link to installed servers and databases. The CapWIN network will enable law enforcement and emergency response groups to communicate with one another over a secure IM system, search multiple databases, and facilitate better coordination between different agencies or officers responding to an emergency. (CNet News.com 21 Aug 2002) http://news.com.com/2100-1001-954809.html

Category 16.3 Infrastructure protection

2002-09-10 infowar information warfare cyberwar infrastructure protection homeland security

NewsScan

#### WORTH THINKING ABOUT: WHY WE REALLY, REALLY NEED COMPUTERS

Resist all those temptations to smash your computer and walk away. Think of where you'd be without it. Michael White, former science editor of British GQ, writes: "Even though most of us can recall a time when digital, modem, and hard drive were not words we thought about or used often, it is difficult to imagine a world without computers. If all the computers in the world shut down tomorrow, we would not simply regress to a time before they were commonplace -- there would be no return to a 1950s lifestyle -- such an event would mark the end of civilization itself. For today we are totally dependent upon computers. The way electricity is delivered to our homes and our factories, the way essential commodities such as gasoline and food reach us is controlled entirely by automated computerized networks. If the world's computers were to shut down, our gas, electricity, and water supplies would soon stop; sewage systems would fail; the financial markets would collapse in disarray; communications would break down; there would be no TV, no radio; military and law-enforcement establishments thrown into confusion; hospitals could function only on a basic level. And from all this, anarchy would soon follow."

Category 16.3 Infrastructure protection

2002-09-18 cybersecurity plan homeland defense infrastructure protection infowar information

NewsScan

#### BUSH ADMINISTRATION PONDERS CYBERSECURITY PLAN

The Bush Administration is considering creating a technology fund, possibly "jointly financed by government and industry," that would "address those "areas that fall outside the purview of both industry and government and yet are critical to the future secure functioning of the Internet." Working papers for the national cybersecurity plan cite the development of highly secure versions of computer operating system software as something that could be paid for by the proposed fund. In addition, the draft documents discuss sweeping new obligations on companies, universities, federal agencies and home users to secure their own "portions of cyberspace." Other ideas under consideration include: improving security of wireless technologies and prohibiting their use in some cases by federal workers; beefing up protection of computer systems that help operate major utilities like water and power; coming up with a game plan for responding to cyberattacks when it's not immediately evident whether the source is a hostile government or a teenage hacker; creating an industry testing center that would ensure software updates don't undermine security measures; and contemplating the creation of a new government network that would handle communications and computing tasks during Internet outages. The White House cautioned that the ideas in the working papers are subject to change until approved by the president, and that any recommendations would still need go through traditional policy and budget processes. (AP 7 Sep 2002) http://apnews.excite.com/article/20020907/D7LT1J980.htm

#### CYBERSECURITY PLAN AUTHORS SEEK FEEDBACK

The White House panel drafting recommendations on beefing up U.S. cybersecurity has decided to open it up for more comment before it is presented to President Bush in two months. "If we just come up with a government strategy and announce it without participation from the people who have to implement it, we're not going to get the level of cooperation? that we need for this," says Bush administration senior cybersecurity advisor Richard Clarke. The National Strategy to Secure Cyberspace offers nearly 60 suggestions on ways that home users, small businesses, universities, large corporations and government agencies can improve cybersecurity, including installing and using security products such as firewalls and antivirus software. However, the draft report backs away from legal action. "We're not creating regulation, not creating mandates," says Clarke. "We want to do this through market forces." (AP 18 Sep 2002) http://apnews.excite.com/article/20020918/D7M4185O1.htm

Category 16.3 Infrastructure protection

2002-10-29 cybersecurity plan homeland defense infrastructure protection infowar information

warfare

NewsScan

#### HOME ISN'T WHERE THE SECURITY IS

Columnist Robert Lemos says the Bush administration's plan to ask home computer users to secure their systems as part of its "National Strategy to Secure Cyberspace" is a misguided effort. Citing the prevalence of users who still call tech support wondering why their computer won't turn on (because they've neglected to plug it in), Lemos says: "The experts are guilty of wrongheaded thinking in relying upon home users to shore up the nation's security. Frankly, that's somebody else's job. Home users are responsible for protecting their own important data. But it's a dangerous illusion to believe they will take better precautions after authorities ask them to upgrade their cyberdefenses." Lemos says the government instead should be focusing on persuading the ISPs "to protect cyberspace from home users. There are simple technologies for doing this. Source egress filtering -- a technique for preventing users from sending data with a false source address, useful in denial-of-service attacks -should be the norm. Companies filter e-mail messages for any viruses and disallow several types of executable attachments; ISPs should do the same." Security expert Dorothy Denning says the only question left is, who will pay? "Once you start formalizing where we are going to put liability, the questions start coming up about who's going to pay for it. And, almost anywhere you put it, the costs are going to end up coming back to the users." (CNet News.com 29 Oct 2002) http://news.com.com/2010-1071-963614.html

Category 16.3 Infrastructure protection

2002-10-30 cyberterrorism infowar information warfare homeland defense infrastructure

protection

NewsScan

#### WARNING OF SIMULTANEOUS CYBER- AND CONVENTIONAL TERRORISM

Rand Corporation's Brian Michael Jenkins told attendees at a security conference in London: "We do not have concrete evidence that terrorists are about to carry out sabotage by coming through cyberspace, but if there's one thing we know: the downside risks of ignoring it exceed the cost of preparation." Acknowledging that terrorists have in the past tended toward bombs and bloodshed, Jenkins indicated that there's an increasing potential for them to coordinate attacks of physical violence with a simultaneous attack on a computer network, and warned: "Such sabotage may become more attractive if the Internet makes it easier to facilitate." (Reuters/San Jose Mercury News 30 Oct 2002)

Category 16.3 Infrastructure protection

2002-11-20 infrastructure protection homeland defense infowar information warfare

cyberterrorism government defenses

NewsScan

#### HOUSE SUBCOMITTE FLUNKS U.S. ON INTERNET SECURITY

A U.S. House of Representatives Government Reform subcommittee has concluded that U.S. Internet security suffers serious problems, especially in the departments of State, Justice and Transportation. The exception to the rule is the Social Security Administration, which the head of the committee called a "shining example of sound leadership and focused attention" on computer security. The most glaring weakness at other agencies is vulnerability against insiders attempting sabotage or trying to profit personally by destroying or stealing sensitive information. And Richard Pethia of the federally funded CERT Coordination Center warned the committee: "Until customers demand products that are more secure or there are changes in the way legal and liability issues are handled, the situation is unlikely to change." (USA Today 19 Nov 2002)

Category 16.3 Infrastructure protection

2002-11-22 homeland security infowar information warfare cyberterrorism infrastructure

protection

NewsScan

#### BY-PRODUCT OF HOMELAND SECURITY IS BUSINESS FOR IT COMPANIES

The creation of the new 170,000-person Department of Security, which among other things will integrate the activities of 22 existing government agencies, will have enormous consequences for information technology contractors, and Harris Miller of the Information Technology Association of America predicts: "The impact is going to be quick and dramatic, and it will provide a lot of opportunities for IT companies." Just a few of those opportunities are: a \$10 billion project by the Immigration and Natural Service to keep track of people entering the U.S.; the creation of an advanced research projects agency, along the lines of the Pentagon's DARPA; and a host of activities required to bring all 22 agencies up to a baseline level of security. (San Jose Mercury News 22 Nov 2002)

Category 16.3 Infrastructure protection

2002-11-25 homeland defense infrastructure protection warning system

NewsScan

#### CALL FOR NEW EMERGENCY WARNING SYSTEM

An expert panel called Partnership for Public Warning comprising members from FEMA, the FBI, the NRC, and the American Red Cross is calling for creation of a high-technology warning system to be placed under the management of the new Department of Homeland Security. The group's chairman, Peter Ward, says: "Our vision is that every person at risk from natural disaster, an accident or terrorism would get a heads-up. Every piece of electronics you own -- be it cell phone, a car phone, a computer a radio, a television -- should have ability to give you a heads-up. It's not hard to think of many scenarios with weapons of mass destruction where, if you get to people right away and tell them to get out of harm's way, you save thousands of lives." (New York Times 24 Nov 2002)

Category 16.3 Infrastructure protection

2002-11-26 homeland defense infrastructure protection education responsibility

NewsScan

SAFE & SOUND IN THE CYBER AGE

Stephen and Chey Cobb, security consultants, remind you that computer security is your patriotic duty:

... "Fellow citizens, now is the time to firewall your broadband connections and filter your email, lest your computer be abused by those who would attack our nation's critical infrastructure. Now is the time to do your patriotic duty and install security patches for your applications, change your passwords, and tighten up those directory permissions. If not, that computer in your den, the one on the high speed Internet connection, could become an attack platform."

Sound a little hokey? Maybe, but we'd be surprised if anyone can find a flaw in the logic or fault any of the stated facts. As far as we are concerned, and we're the ones who've been giving this speech, the large and growing number of unprotected, high-powered, always-on, broadband-connected personal computers does indeed represent a threat to the national infrastructure (note that we are both U.S. citizens, but this is by no means a uniquely American perspective -- we would be holding the same truths to be self-evident if we were citizens of the United Kingdom, or Germany, or Brazil, or anywhere else that is experiencing a rapid increase in broadband connectivity).

We have had these thoughts, and said these things, for some time, but we feel compelled to reiterate them now, because our President has just signed the Homeland Security Bill, causing the biggest overhaul of the U.S. government since the National Security Act of 1947 unified the Armed Forces under a single department and created the National Security Council and Central Intelligence Agency. The Homeland Security Department is expected to have a combined workforce of more than 175,000 employees and pull together more than 20 agencies. As if that wasn't enough for one bill, the Homeland Security Act also amends a bunch of other laws and encompasses things like the creation of a new form of charitable trust to "provide for the spouses and dependents of military, CIA, FBI and other federal employees killed in the line of duty in the war on terrorism." A noble goal, but arguably extraneous to the creation a new department of government. We will have more to say about the Homeland Security Act in future columns, after we have more completely digested all 470 pages (okay, that's the double-spaced version, but still, this is not light reading).

What we want to highlight here is the starring role that computer security plays in this legislation. For a start, the bill includes a definition of information security and spells out that other C-I-A, the one that infosec people have been working at for years: Confidentiality, Integrity, and Availability. In a dramatic turn, the bill makes significant amendments to the Computer Fraud and Abuse Act of 1986. Indeed, these amendments are to be known as the "Cyber Security Enhancement Act of 2002." The "enhancements" include increased penalties for criminal hacking, up to life imprisonment "if the offender knowingly or recklessly causes or attempts to cause death" through conduct such as intentionally accessing a computer without authorization or exceeding authorized access.

What we don't see in the Homeland Security Bill, or in the \$900 million appropriation for computer security research that was also passed last week, is funding for the education of network computer users and operators. These are the people, like you, and us, and generations just getting started, who are connecting their computers to the Internet. The connections are often high bandwidth (24 million Americans have broadband Internet connections at home according to Pew report this summer).

Whose job is it to tell the people who have these connections that their computer could unwittingly host a distributed denial of service attack? Who is responsible for telling computer owners to make sure they are not harboring programs that could bring down emergency service communications during a terrorist attack? When you get a Dell does it say on the box: "Dude, this thing could kill someone"? No, and we don't expect to see such a warning sticker any time soon. That is the point. With powerful technology comes a ton of responsibility. But it tends to arrive somewhat later than the technology itself.

In the meantime, securing all those computers on the network will take some serious motivation. Patriotism seems like a good place to start.

... Chey Cobb, the author of "Network Security for Dummies," is an independent consultant and former senior technical security advisor to the NRO and can be reached at chey@patriot.net. Stephen Cobb, the author of "Privacy for Business: Web Sites and Email," is Senior VP of Research and Education for ePrivacy Group and can be reached at scobb@cobb.com.

Category 16.3 Infrastructure protection

2002-12-13 cyberterror homeland defense infowar information warfare critical infrastructure

study analysis prediction

#### NewsScan

#### IDC'S CRYSTAL BALL SEES CYBERTERROR IN THE FUTURE

Research firm IDC has released its list of prognostications for 2003, and high on its list is a prediction that a major cyberterrorism event will occur, disrupting the economy and crippling the Internet for a day or two. "The war with Iraq will galvanize hackers," says John Gantz, chief research officer for IDC. On the sunnier side, IDC forecast: a 6% rise in spending on information technology and telecommunications, a rebound in sales of midrange server computers; and a boost in Linux's market share at the expense of Unix. "We're saying that Linux will eat Unix," says Gantz. Other predictions include: a stagnant or shrinking IT services market as companies scale down project size and turn to IT outsourcing; a booming wireless LAN market, which will delay the introduction of so-called third-generation wireless communications networks; and a 27% increase in online messaging, with the total number of e-mail messages sent each day rising 30% to 40 billion a day. "There will be more spam in your life," says Gantz. (CNet News.com 12 Dec 2002) http://news.com.com/2100-1001-977780.html

Category 16.3 Infrastructure protection

2002-12-20 national strategy cyberspace security homeland defense cyberterrorism infowar

information warfare ISP Internet service providers privacy monitoring viruses

infrastructure protection privacy

#### NewsScan

#### PROPOSED NATIONAL STRATEGY TO SECURE CYBERSPACE

The President's Critical Infrastructure Protection Board is planning to propose that Internet service providers be required to help build a centralized monitoring system that could be used to protect network users from both computer viruses and terrorist attacks. The plan would be part of an Internet strategy for the new Department of Homeland Security. Some technology company executives say they fear that the system could be used to invade individual privacy but Tiffany Olson, chief of staff for the Board, says that the plan will not require gathering data that would allow monitoring at an individual user level. She says a centralized monitoring system is needed because, currently, "we don't have anybody that is able to look at the entire picture. When something is happening, we don't know it's happening until it's too late." (New York Times 20 Dec 2002)

#### GOVERNMENT VOWS TO RESPECT CITIZEN PRIVACY

Responding to concerns that the Internet monitoring center proposed by the government's forthcoming report "National Strategy to Secure Cyberspace," President Bush's top cyberspace adviser, Richard Clark, says that the plan contains nothing which "in any way suggests or proposes a government system that could extend to monitoring individuals' e-mails"; to the contrary, it "articulates a strong policy of protecting citizens' privacy in cyberspace." The Bush administration contemplates that any Internet monitoring operation would be run by the private sector and not the government. There is no proposal for monitoring e-mail or other data traffic of Internet users. (20 Dec 2002)

# 16.4 Military & government perspectives on INFOWAR

Category 16.4 Military & government perspectives on INFOWAR

2002-02-14 information warfare critical infrastructure protection counterattack response military

action policy prediction

NewsScan

Category 16.4

#### RESPONSE TO CYBERATTACK ON U.S. COULD INCLUDE MILITARY ACTION

White House technology advisor Richard Clarke told a Senate Judiciary subcommittee that a cyberattack on the United States would be answered "in any appropriate way: through covert action, through military action, any one of the tools available to the president." Clarke pointed out that a serious cyberattack is almost inevitable from the nation's enemies, because it is cheaper and easier than a physical attack. Senator Charles Schumer (D, NY) pointed out the potentially serious consequences of a successful attack over the Internet: "A well-planned and well-executed cyberattack wouldn't just mean the temporary loss of e-mail and instant messaging. Terrorists could gain access to the digital controls for the nation's utilities, power grids, air traffic control systems and nuclear power plants." (AP/USA Today 14 Feb 2002) http://www.usatoday.com/life/cyber/tech/2002/02/14/cyberterrorism.htm

2002-03-11 reliability availability battlespace information warfare operating system palmtop

Military & government perspectives on INFOWAR

handheld

RISKS, http://www.newscientist.com/news/news.jsp?id=ns99992005 21 94

David Wagner in RISKS: "\*New Scientist\* is reporting that the US military is planning to deploy palmtops for ground troops to use in transmitting targeting information for air strikes and the like. The application software will be running on top of Windows CE."

Category 16.4 Military & government perspectives on INFOWAR

2002-03-11 military battlefield information warfare battlespace availability reliability

RISKS, http://insideout.wbur.org/documentaries/reshapingmilitary/ 21 94

Reports from the US Army indicated that new battlefield computers would be used to help soldiers receive battlespace data. An executive officer was quoted on a radio program as saying, "We use nothing but Windows NT systems, that are hardened, to provide HTML products, which are nothing but homepage products, to disseminate the information via regular Internet protocols." Commented a RISKS correspondent, "Gives new meaning to 'Blue Screen of Death' ".

Category 16.4 Military & government perspectives on INFOWAR

2002-04-22 information warfare infowar asymmetrical communications consolidation

cooperation hardening networks

Security Wire Digest 4 31

\*ARMY UNITS JOIN FORCES IN IT NETWORK DEFENSE By Cheryl Balian

The U.S. Army's institutional and tactical divisions, as well as other defense agency partners, are stepping up plans to develop a fully consolidated and more secure computer network.

Military units such as the Space and Missile Defense Command, the Defense Information Systems Agency, and the U.S. Army Signal Command are making the changeover, entitled "The Mannheim Project," a priority as part of a larger information technology merger. The centralized network is designed to provide increased security against asymmetrical warfare that may target the Department of Defense's (DoD) information systems.

"Much greater collaboration is needed," says Lt. Gen. Robert W. Noonan, Jr., the Army's deputy chief of staff for intelligence. The technological framework of government and military agencies like the DoD is considered a ripe target for attacks that could target anything from tactical and personnel information to the network's structure, he adds.

One of the first stages of this informational movement is occurring at the Army Signal Command, which is transforming its operations and will become known as the Network Enterprise Technology Command (Netcom). Netcom will be charged with overseeing and managing day-to-day operations for all of the Army's IT systems and networks. Netcom will also provide regular situation reports to the Army's CIO beginning May 1, but formally launches in October.

One expert cites private industry as a useful role model for securing military and government IT systems, because large companies tend to operate under a framework of free-flowing information and interoperability.

"(The military) should tap into that," said Gilman Louie of In-Q-Tel, a venture capital vehicle established by the Central Intelligence Agency. "They are going to have to deal with industry anyway if they're going to face asymmetrical warfare." Louie stressed that the Army needs to take advantage of the IT processes--including the information sharing model--and infrastructure established by the corporate world to maximize security.

Category 16.4 Military & government perspectives on INFOWAR

2002-05-05 information warfare cyberattacks international infowar

RISKS, http://www.latimes.com/news/nationworld/world/la-042502china.story 22 05

In May 2002, reports surfaced about U.S. intelligence on Chinese military efforts to launch wide-scale cyber-attacks on American and Taiwanese computer networks, including Internet-linked military systems considered vulnerable to sabotage.

Category 16.4 Military & government perspectives on INFOWAR

2002-06-04 battlespace information warfare infowar

FindLaw Download This 88

#### WEB SITE AIDS AFGHAN WAR EFFORTS

The war in Afghanistan is going online. A drab tent under the Afghan sun hides a high-tech war room that soon will become the nerve center of the campaign: Inside, tables are lined with soldiers bent over laptops. . . All are logged onto the Tactical Web Page, a secret, secure website being used in combat for the first time, through which American commanders at Bagram air base and in the United States can direct the fight in Afghanistan.

http://news.findlaw.com/ap/ht/1700/5-30-2002/20020530054502\_28.html

Special Coverage: War On Terrorism

http://news.findlaw.com/legalnews/us/terrorism/index.html

Category 16.4 Military & government perspectives on INFOWAR

2002-11-15 infowar information warfare intelligence surveillance spying

NewsScan

#### WHAT IS NRO?

NRO, or National Reconnaissance Office, was mentioned in Stephen and Chey Cobb's "Safe & Sound in the Cyber Age" column in NewsScan the other day, and some of readers asked for more information about it. Here is Stephen's elaboration on the topic: Although many Americans have never heard of it, the NRO is probably the biggest of all the U.S. intelligence agencies in terms of dollars spent. Until the '90s the government repeatedly denied the existence of the NRO, which was established by Eisenhower. Some people think the agency would still be secret today if it had not decided to build a very visible \$300-million headquarters on the edge of Dulles airport. Serving as the collector of intelligence data, via satellites, spy planes, and other means, the NRO does not have as many direct employees as the slightly better known National Security Agency (with 20,000 workers, the NSA is the largest employer in Maryland). And the NRO budget, publicly listed at \$6 billion per year, appears to be less than that of the NSA. But a lot of NSA/CIA/USAF personnel actually work at the NRO, together with a huge band of contractors. And the director of the NRO just happens to control the Pentagon's \$68-billion space budget. Remember when a Titan 4 rocket exploded shortly after launch from Cape Canaveral in 1998? The NRO satellite it was carrying was reported to be worth \$1 billion. That was only one of many such, not to mention planes, drones, etc. They all generate huge amounts of traffic requiring highly complex networks and massive computing power to handle and digest. Chey Cobb worked on securing those networks and computers. Note that all of the above is unclassified. Here are links to 2 views of the agency: Official:

http://www.nro.gov/index1.html Unofficial:

http://www.fas.org/irp/eprint/thompson.html Also note that the unofficial view, while generally critical of the agency, points out recent advances in security as one area of improvement.

# 16.5 Hacktivism

Category 16.5 Hacktivism

2002-05-20 hacktivisists investigation Web vandalism defacement arrests confidentiality penetration probation juvenile

Security Wire Digest, SecurityFocus; http://online.securityfocus.com/news/414 4

Hacktivists calling themselves the Deceptive Duo were arrested in May after an FBI investigation. Using handles "Pimpshiz" and "The Rev," the pair vandalized dozens of Web sites supposedly to stress the importance of improving security in the face of international threats to the USA's infrastructure. In one case, the pair posted a page apparently stolen from a bank system that showed customer names and account numbers.

Robert Lyttle, 18, was ordered into house arrest for having violated the terms of his probation for a previous hacking conviction only four months prior to the latest alleged crimes. In the previous conviction, Lyttle had defaced more than 200 Web sites, replacing them with pro-Napster e-graffiti and had been ordered to serve 90 hours of community service and was barred from hacking and from using pseudonyms online. As an 18-year-old, Lyttle faced federal charges instead of juvenile court this time. Little information was made available by the FBI about the second hacker suspected in the case.

Category 16.5 Hacktivism

2002-10-03 Web hijacking cult politics repression

NewsScan

#### NEWSPAPER SITE REROUTED TO FALUN GONG

Surfers who tried to visit the site of the Hong Kong newspaper Mingpao were diverted to another site filled with messages about Falun Gong, the organization of a meditation group that is outlawed in mainland China and described by Chinese officials as an "evil cult." A Falun Gong spokesman in Hong Kong denied the organization was responsible for the vandalism: "Just because the users are redirected to the Falun Gong Web site doesn't mean Falun Gong did it. We suspect others are trying to frame Falun Gong with these kinds of tricks. In a free and open society, you don't have to resort to these tactics." (AP/New York Times 3 Oct 2002)

Category 16.5 Hacktivism

2002-12-18 hacktivism harassment invasion privacy denial-of-service attacks spam e-mail

NewsScan

#### WEB ACTIVISTS GO AFTER RALSKY AND POINDEXTER

Web activists have uncovered the home address and phone numbers for government surveillance head John Poindexter and bulk spammer Alan Ralsky, and have posted the information on more than 100 Web sites. The action has led to Ralsky being deluged with junk mail and Poindexter undergoing the scrutiny that every American soon will experience. An article in the Detroit Free Press quoted Ralsky as complaining, "They're harassing me," after anti-spammers signed him up with as many direct mail agencies as possible. In Poindexter's case, his home address, complete with satellite photos, has been published online as well as his phone number and those of his neighbors. That's actually just a small portion of the personal information the U.S. government plans to collect under Poindexter's Total Information Awareness program, which will compile credit card, medical, travel, school and other records in an effort to spot terrorists. (BBC News 16 Dec 2002) http://news.bbc.co.uk/2/hi/technology/2580089.stm

39

# 17.1 Penetration

Category 17.1 Penetration

2002-01-20 database vulnerability contest advertising hackers attack testing penetrations

vulnerabilities

Security Wire Digest 4 5

#### ORACLE "UNBREAKABLE" BOAST BEING TESTED

Oracle's "Unbreakable" advertising campaign is about to be broken, say industry experts. Following Oracle's boastful marketing campaign that kicked off in September, hackers began blasting away at the company's code, resulting in a tenfold surge in hacking attempts. Though Oracle says none of the attempts were successful so far, a presentation scheduled for early February may soon change that. According to SecurityFocus, U.K. security researcher David Litchfield will reveal "a suite of at least seven vulnerabilities currently in the company's patch pipeline." Some security experts have said that these vulnerabilities change the claim of "unbreakable" from marketing hype to a false sense of security.

Category 17.1 Penetration

2002-02-20 physical security Windows share network compromise confidentiality control

penetration

RISKS 21 92

Greg Searle posted a cautionary note warning novice users about the importance of preventing access to their workstations when they step away from their desks. He pointed out that it takes only seconds to set the share property of a drive to allow total access from anywhere in the network. No one would ever know that the share had been changed or who changed it. Lock down your machine before leaving it. On a Windows 2000 or Windows NT machine, it's as simple as hittling CTL-ALT-DEL and clicking on LOCK.

Category 17.1 Penetration

2002-02-27 penetration confidentiality cracking criminal hacker consultant Social Security Number SSN vulnerabilities holes demonstration ethics professional standards

NewsScan

# SECURITY CONSULTANT SAYS HE HACKED NYT COMPUTERS [27 Feb 2002]

Adrian Lamo, a 20-year-old part-time security consultant in San Francisco, claims to have hacked the Web site of the New York Times and browsed through the names and Social Security numbers of the newspaper's employees, customers, and editorial contributors. Lamo says he notified the newspaper of what he had done -- and that the Times has patched up the security holes but has not acknowledged that he penetrated its system. (AP/San Jose Mercury News 27 Feb 2002) http://www.siliconvalley.com/mld/siliconvalley/2752998.htm

In September, an article in the New Scientist reported, "A computer security expert has revealed how he altered news articles posted to Yahoo!'s web site without permission. The incident highlights the danger of hackers posting misleading information to respected news outlets. Freelance security consultant Adrian Lamo demonstrated that, armed only with an ordinary Internet browser, he could access the content management system used by Yahoo!'s staff use to upload daily news. He added the false quotes to stories to prove the hole was real to computer specialist site Security Focus. Yahoo! has issued a statement saying the vulnerability has been fixed and security is being reviewed. But experts say that the incident demonstrates a serious risk. "Just think how much damage you could do by changing the quarterly results of a company in a story," says J J Gray, a consultant with computer consultants @Stake."

http://www.newscientist.com/news/news.jsp?id=ns99991329

Category 17.1 Penetration

2002-04-22 criminal hackers fraud penetration data corruption

RISKS 22 04

Peter G. Neumann wrote:

>A group of Chicago Web site operators say they will break into school, government and corporate computers and alter records, for fees starting at \$850. But at least one security expert thinks the operation probably is a scam. Among the services promised by Chicago-based 69 Hacking Services, is changing bad grades and other records on elementary, high school or college computer systems. [Source: Brian McWilliams, Newsbytes, http://www.newsbytes.com/news/02/]<

Category 17.1 Penetration

2002-04-22 Internet banking penetration data theft confidentiality Web breakin crackers

criminal hackers

Security Wire Digest 4 31

#### FLORIDA BANK BREACH NETS ONLINE BANKING DATA

A cracker managed to breach a Florida bank's firewall and steal the personal data of 3,600 online-banking customers. Officials at Republic Bank--among the first in the state to offer Internet banking in 1996--discovered the incident a few weeks ago but kept it from customers until April 17. The theft came to light after the attackers contacted the bank, whose main Web site runs Microsoft's IIS 4.0 and is hosted by Advances.com of Fort Lauderdale. No accounts were accessed during the attack, the bank reports. The FBI is investigating and Republic Bank has contracted a team of security consultants to review its systems.

Category 17.1 Penetration

2002-04-25 crimina hacking bank penetration data theft automated teller machine ATM trial

conviction prison sentences

Security Wire Digest 4 32

#### RUSSIAN ATM CRACKERS SENT TO PRISON

Two leaders of a Russian hacker group received five-year prison sentences for their roles in stealing almost a million dollars from foreign bank accounts after manipulating automatic teller machines (ATM) in Moscow. More than 6,000 people were victims of the thefts, according to a news report. Zviadi Beria and Vladimir Medvedov, who adamantly denied their guilt, were each sentenced to five years in prison. The group's main organizer, Yuri Levashov, cooperated with authorities and received a three-year sentence, with immediate release due to a special arrangement. Four others were given three-year suspended sentences.

Category 17.1 Penetration

2002-05-05 penetration confidentiality data leakage Web defacement management response

RISKS 22 05

Midwest Express Airlines distributed the following announcement about a hack:

On the morning of Monday April 22, Midwest Express Airlines was informed that customer profile data had been published on the Internet, specifically on the U.S. Space and Naval Warfare Systems Command Web site. The data published contained a handful of user profiles including names and e-mail addresses. This screenshot of data was captured from the Midwest Express test server, not the actual Web site. This test server is used for testing new enhancements to www.midwestexpress.com.

Midwest Express has always taken steps to ensure security. As a result of this situation, a number of additional precautionary measures were taken to ensure that customer data was protected:

Since all passwords have been changed, the next time you visit midwestexpress.com and login to your profile, you will be prompted to change your own password upon successfully answering a challenge/response question that you created.

While Midwest Express is confident in the security of its Web site, we are always assessing our Web site for potential vulnerabilities and taking appropriate steps when needed. We assure you that your customer information, purchases and other transactions are secure.

<sup>\*</sup> The U.S. Space and Naval Warfare Web site immediately removed the defaced Web page from the Internet.

<sup>\*</sup> A security company was contracted to eliminate any vulnerability to our test server.

<sup>\*</sup> All customer passwords to Web profiles were changed to protect and restrict access to the customer data.

Category 17.1 Penetration

2002-05-17 credit report confidential personal data identity theft penetration criminal hackers

NewsScan; http://www.nytimes.com/2002/05/17/technology/17IDEN.html

#### CREDIT REPORTS STOLEN FROM EXPERIAN DATABASE

Network vandals have stolen 13,000 credit reports in recent months from Experian, a national reporting agency. An Experian executive said, "I've never seen anything of this size. Privacy is the hallmark of our business. We're extraordinarily concerned about the privacy issue here, and the trust factor." The intruders used an authorization code from Ford Credit to obtain the reports, which gave the intruders access to each victim's personal and financial information, including address, Social Security number, bank and credit card accounts and ratings of creditworthiness. Ford has sent letters via certified mail to all 13,000 people, urging them to contact Experian and the two other major credit reporting companies, Equifax and TransUnion, and to report any evidence of abuse to the FBI. (New York Times 17 May 2002)

Penetration Category 17.1

2002-05-27 criminal hackers penetration state database financial information SSN

22 10 RISKS, FINDLAW

Computer hackers have cracked into the state's personnel database and gained access to financial information for all 265,000 state workers, including Governor Gray Davis, officials said Friday [May 2002]. The database, housed at state's Teale Data Center in Rancho Cordova, holds names, Social Security numbers, and payroll information for everyone from office workers to judges. Authorities said that so far they have found no evidence that the information has been used illegally. <a href="http://www.sfgate.com/cgi-in/article.cgi?file=/chronicle/archive/2002/05/25/MN179392.DTL">http://www.sfgate.com/cgi-in/article.cgi?file=/chronicle/archive/2002/05/25/MN179392.DTL</a>

Category 17.1 Penetration

2002-08-14 criminal hacking university officials industrial espionage penetration policy

punishment ethics

#### NewsScan

#### YALE ACCUSES PRINCETON OF HACKING INTO ADMISSIONS RECORDS

Princeton University has admitted that its admissions personnel hacked into rival Yale's computer system to check on the applications status of 11 students who also had applied to Princeton. The university has suspended with pay its associate dean and director of admissions, and a spokeswoman expressed deep regret "that information provided by students in good faith to the university was used inappropriately by at least one official in our admissions office." The perpetrator(s) apparently were easily able to access the students' records via the publicly available Yale.edu Web site because they already had the students' passwords -- the names, Social Security numbers and dates of birth they had provided on their Princeton applications. The site had been set up with a feature that enabled students to check on the status of their applications themselves. The founder of one electronic-rights group noted that while Princeton's actions clearly were wrong, it was foolish of Yale to rely on Social Security numbers and birth dates to secure student data. "It's not enough to have a weak Web site and depend on the good ethical behavior of others not to penetrate it," he said. "Similarly, it is not adequate to say that just because you found the weak Web site you should go ahead and penetrate it." (Wall Street Journal 26 July 2002)

# PRINCETON'S PUNISHMENT FOR COMPUTER VANDALS

Princeton University has decided on the punishment for two Admissions Office officials responsible for the invasion of Yale University's computer system to obtain applicant files: the one who actually did the breaking in will be transferred to another job, and the dean to whom he reported will be allowed to retain his position until his scheduled retirement next June. Princeton president Shirley M. Tilghman says the university has learned from this episode of computer vandalism: "One of the lessons of this experience is that even individuals with a high degree of sensitivity to ethical principles in traditional settings can fail to be equally sensitive when technology is involved," she said, "as when someone who would never open a sealed envelope addressed to another person enters a secured Web site." (New York Times 14 Aug 2002)

Category 17.1 Penetration

2002-08-23 penetration criminal hackers stupidity legal liability unauthorized access computer fraud abuse investigation

#### NewsScan

#### SECURITY FIRM SEEKS ATTENTION, GETS MORE THAN IT HOPED FOR

ForensicTec Solutions, a new computer security company in San Diego, sought publicity by bragging to the Washington Post that it had used free software to break into Army, Navy and NASA computers to demonstrate their security vulnerabilities. Big mistake, because when the FBI learned of the intrusions it raided the firm's offices. Mark Rasch, the Justice Department's former top computer crimes prosecutor, explained: "Just because you can break into Army computers doesn't mean you either should do it, have a right to do it, or can avoid criminal liability for doing it. They thought they were doing a public service. What they did, at best, was exercise a monumental lack of judgment." (AP/Washinton Post 22 Aug 2002)

Category 17.1 Penetration

2002-09-26 criminal hacking legislation proposed law bill intellectual property piracy inspection

monitoring penetration

NewsScan

## HACKING BY ANY OTHER NAME

A new debate in Congress over legislation proposed by Howard Berman (D-Calif.) will have to struggle to find a definition of the word "hacking." Berman's bill would give the recording industry the right to use network software to inspect people's personal computer files to make sure they do not contain copyrighted music. The congressman says there is "no question" that the "vast majority" of peer-to-peer downloads constitute copyright infringement, but opponents of the Berman bill say it goes too far in invading the rights of individuals. Wayne State University professor and computer security expert Jessica Litman says of the proposed legislation: "What it seems to say is that if the copyright owner doesn't impair the integrity of files, it gets a complete free pass, and if it does impair the integrity of files, it gets a qualified cheap pass." Stan Lebowitz, a management professor at University of Texas-Dallas, comments: "Spoofing seems like a legitimate technique for them to use. Hacking, however, seems to go to far" — and notes that what the bill allows "would still qualify as hacking, under most laws and in most people's minds." (USA Today 25 Sep 2002)

http://www.usatoday.com/tech/news/techpolicy/2002-09-25

# 17.3 Phreaking

Category 17.3 Phreaking

2002-03-05 phone phreaking fraud unauthorized charges

RISKS, http://www.computerworld.com/cwi/story/0,1199,NAV47-

74\_STO68446,00.html

As mentioned in RISKS by Anthony W. Youngman and summarized by Peter G. Neumann, Nicholas Petreley suffered from phone phreaking and reported on it extensively in his \_Computerworld\_ column

<http://www.computerworld.com/cwi/story/0,1199,NAV47-74\_STO68446,00.html >. Neumann wrote, "After noticing the frequent calls to Germany, Nick canceled his calling card and switched his long-distance carrier. The person who had been piggybacking on his old card then managed to switch his new account back to the old carrier and make more calls. It turns out that person had created a Web account for him, so that he no longer received statements. The entire saga is a real horror story, and very well worth reading. Lots of lessons to be learned."

Category 17.3 Phreaking

2002-05-14 cell phone wireless clone fraud differential cryptanalysis

NewsScan

#### ATTACK OF THE PHONE CLONERS

A team of engineers from IBM and the Swiss Federal Institute of Technology have found a way to capture the data necessary to "clone" a cell phone in 60 seconds. Previous methods used to copy the identifying data that enables calls to be charged to another person's phone took about eight hours. The researchers found that they could gain valuable information about the numerical "key" a phone uses to uniquely identify its owner by timing how long the phone's chip took to complete certain tasks and by measuring changing current flows across the chip. Taken together, the information revealed what was being done to the numerical key. The researchers say that chips can be protected against this type of espionage by making sure all computational tasks take the same amount of time, or by changing the way a chip carries out certain computations. (BBC News 14 May 2002) http://news.bbc.co.uk/hi/english/sci/tech/newsid\_1984000/1984887.stm

93

# 18.1 Theft

Category 18.1 Theft

2002-08-23 laptop computer theft loss tracking software Internet

NewsScan

#### FIND THAT LAPTOP! NEW TRACKING SOFTWARE FOR NOTEBOOKS

In response to an epidemic of laptop thefts, leading notebook makers IBM, Hewlett-Packard and Dell are offering software with their new machines that enable tracking as soon as their connected to the Internet. IBM, which offers ComputracePlus software from Absolute, says it's seeing growing demand from laptop customers in the education and enterprise markets. Service costs start at \$49 for a 12-month license for a single computer. The tracking-agent software imperceptibly connects to Absolute's monitoring center whenever its user connects to the Internet. If the notebook is reported stolen or lost, its location is tracked and local law officials are called in to retrieve it. Although popular, this approach to laptop security does have some weaknesses. "A lot of people steal laptops for commercial espionage -- to get the data that resides on them," says an IDC analyst. "Those people will steal them without ever intending to go online." In other cases, a thief could reformat and configure the hard drive in a way that bypasses the tracking agent. "We'll survive a reformat of the hard drive, but where it gets tricky is when people reinstall operating systems on top of each other," says Absolute CEO John Livingston. Experts say this type of tracking system works best if it is part of a larger theft-prevention strategy that includes cable locks or motion-sensitive alarms. (CNet News.com 22 Aug 2002)

http://news.com.com/2100-1040-954931.html?tag=fd\_top

# 18.2 Loss

Category 18.2 Loss

2002-08-16 laptop computer losses internal controls policies

NewsScan

#### DETAILS, DETAILS: IRS LOSES COMPUTERS (EXACT NUMBER UNKNOWN)

An Inspector General's report has concluded that the Internal Revenue Service has lost (or had stolen) some unspecified number of personal computers that had been lent to volunteers who were assisting low-income, disabled, and senior citizens prepare their tax returns. IRS critic Sen. Charles E. Grassley (R-Iowa) wrote in a letter to the federal Office of Management and Budget: "I'm worried that just as clothes dryers have the knack of making socks disappear, the federal government has discovered a core competency of losing computers." An IRS spokeswoman said that the agency has been working "for some time" to improve its internal controls over the computers it lends to volunteers, and "will continue" to do so. (Washington Post 16 Aug 2002)

# 19.1 Software piracy

Category 19.1 Software piracy

2002-02-28 music software piracy intellectual property theft shoplifing data storage connectivity

NewsScan

#### HAVE IPOD, WILL SHOPLIFT?

It turns out that Apple's new iPod device is well-suited to electronic shoplifting, with its roomy 5GB hard drive capable of serving as portable storage for very large files, such as the latest Mac OS. A CompUSA shopper describes watching a young man equipped with an iPod walk over to a nearby display Macintosh, plug his iPod into the machine with a FireWire cable, and copy Microsoft's new Office for OS X suite, which retails for \$500. The whole process took less than a minute. "Watching him, it dawned on me that this was something that was very easy to do," said witness Kevin Webb. "In the Mac world it's pretty easy to plug in and copy things. It's a lot easier than stealing the box." And while the iPod has a built-in anti-piracy mechanism that prevents music files from being copied, there are no such protections for software. "This is the first we have heard of this form of piracy," said a Microsoft product manager. "And while this is a possibility, people should be reminded that this is considered theft." (Wired.com 28 Feb 2002) http://www.wired.com/news/mac/0,2125,50688,00.html

Category 19.1 Software piracy

2002-04-19 software piracy intellectual property copyright violations counterfeit arrests police

international

NewsScan

#### RAIDS ON SOFTWARE PIRACY RING

More than 125 FBI and state and local enforcement officers in California arrested 27 people, mostly Taiwanese [nationals], in Freemont, San Jose, and Union City, charging them with participation in an international software piracy ring that has cost Microsoft \$75 million in lost sales of its software products. The ring has been under police surveillance for more than two years. (San Jose Mercury News 18 Apr 2002)

http://www.siliconvalley.com/mld/siliconvalley/3093841.htm

Category 19.1 Software piracy

2002-05-21 software piracy criminal gangs sentence prosecution intellectual property copyright

FindLaw Download This 86

# INTERNET SOFTWARE PIRACY GROUP HEAD SENT TO PRISON

The leader of "DrinkorDie," one of the oldest and largest international software piracy rings on the Internet, was sentenced on Friday to three years and eight months in prison for conspiring to commit copyright infringement, U.S. officials said. They said John Sankus, 28, of Philadelphia, whose screen name was HellFire spelled backward, received the sentence as part of plea agreement reached with prosecutors in February. Prosecutors have described DrinkorDie as a highly structured, security-conscious group that illegally reproduced and distributed hundreds of thousands of copies of copyrighted works around the world.

http://news.findlaw.com/news/s/20020517/crimetechdc.html

FindLaw's Computer Crime Publications

[Copy and paste link into browser]

http://www.findlaw.com/01topics/10cyberspace/computercrimes/publications.html

Category 19.1 Software piracy

2002-10-23 copyright intellectual property software piracy Asia

NewsScan

# SOFTWARE PIRACY IN ASIA

Microsoft senior corporate attorney Katherine Bostick says that software piracy is increasing throughout the world and especially in Asian countries such as China, Taiwan, Hong Kong, Malaysia and Indonesia. "It involves organized crime," says Bostick. "When you are dealing with high-end counterfeits, you are talking about organizations that have a full supply chain, a full distribution chain, full manufacturing tools all in place, and it is all based on profits." How bad is the situation? "Two out of five business software applications were pirated in 2001, which is the second consecutive year that the piracy rate has increased." And why is it happening? "Right now, the cost of violating intellectual property rights is not that high. There is really no penalty for that major person and they will be right back in business the next day or the next month." (Reuters/San Jose Mercury News 23 Oct 2002)

# 19.2 Music piracy

Category 19.2 Music piracy

2002-01-10 music copyright intellectual property marketing distribution subscription

NewsScan

#### NAPSTER GETS READY FOR REBIRTH AS SUBSCRIPTION SERVICE [10 Jan 2002]

Napster, the Internet file-swapping service that was plagued by lawsuits accusing it of violating the intellectual property rights of music producers and artists, has launched a new six-week trial in which 20,000 volunteers will swap music files legally. The company will offer 50 downloads per month for about \$5-10, and will be using improved file identification technology. A Napster spokesman says the company is "close to getting all major label content." (AP/New York Times 10 Jan 2002) http://www.nytimes.com/aponline/technology/AP-Napster.html

Category 19.2 Music piracy

2002-01-24 music peer-to-peer networking copyright infringement bootleg intellectual property

rights infringement lawsuit judgement

#### NewsScan

#### NAPSTER LAWSUIT ON HOLD WHILE PARTIES RECONSIDER SETTLEMENT [24 Jan 2002]

U.S. Federal District Judge Marilyn Patel has granted a request by Napster and four record companies to suspend for 30 days the lawsuit brought by the record industry charging Napster, the Internet music-swapping service, with illegal distribution of copyrighted material. The four record companies joining Napster in the request were AOL Time Warner, BMG, Vivendi Universal and Sony; a fifth company, EMI, declined to participate in the request. Napster is gradually transitioning itself from a free to a paid-subscription service, and Hilary Rosen of the Recording Industry Association of America says of Napster: "We understand they have limited their repertory to licensed music. Resolving the lawsuit may now be feasible." (New York Times 24 Jan 2002)

http://partners.nytimes.com/2002/01/24/technology/ebusiness/24NAPS.html

Category 19.2 Music piracy

2002-02-26 intellectual property music piracy e-commerce

NewsScan

#### RIAA: PUT ANOTHER NICKEL IN THAT NICKELODEON FOR MUSIC, MUSIC, MUSIC

The music industry is desperate to find a way of downloading a solution to the problem of illegal downloading of copyrighted songs. The Recording Industry Association of America (RIAA) says that shipments by record companies to consumers have dropped by more than 10% in the past year, and RIAA president Hilary Rosen complains: "When 23% of surveyed music consumers say they are not buying more music because they are downloading or copying their music for free, we cannot ignore the impact on the marketplace. " (Reuters/New York Times 25 Feb 2002) http://partners.nytimes.com/reuters/technology/tech-leisure-music.html

Category 19.2 Music piracy

2002-02-28 music peer-to-peer networking copyright intellectual property rights infringement

lawsuit judgement service alternative

# NewsScan

## SONY LICENSES MUSIC TO SONG-SWAPPING SERVICE [28 Feb 2002]

Peer-to-peer music-swapping service CenterSpan Communications says it's clinched a deal to distribute Sony Music Entertainment songs, marking the first time a major record label has licensed its content to a file-sharing outfit. CenterSpan bought the file-swapping Web site Scour.com after it declared bankruptcy in 2000. The pact calls for CenterSpan to pay Sony about \$2 million in cash plus 283,556 shares and a warrant to buy 189,037 additional shares at \$8.11 per share. A CenterSpan spokesman said the company is also talking to other record labels and movie studios, as well as online music subscription services such as Pressplay. "The deal continues the experimental phase the music industry is going through as it tries to figure which digital distribution model is going to work," says a GartnerG2 analyst. (Reuters 28 Feb 2002)

http://story.news.yahoo.com/news?tmpl=story&cid=581&u=/nm/20020228/tc\_nm/media\_centerspan\_sony\_dc\_1

Category 19.2 Music piracy

2002-05-06 intellectual property P2P peer-to-peer file sharing music download piracy sales

surveys

NewsScan

#### DOES FREE ONLINE MUSIC MAKE FANS WANT TO BUY?

The market and consumer research firm Jupiter Research has issued a report reports that, contrary to what the music industry thinks, music file-sharing networks such as Kazaa and Music City are actually good for business: "File-sharing is a net positive technology", says the report, because "it gets people enthusiastic about new and catalog music." But not so fast there. Hart Research Associates, in a study prepared in November for the Recording Industry Association of America, came to just the opposite conclusion: "People who love music and buy it and who also use file-sharing services would be buying more of it were it not for the availability of free music online." The correct answer? Pay your money and take your choice. (New York Times 6 May 2002)

http://partners.nytimes.com/2002/05/06/technology/06MUSI.html

Category 19.2 Music piracy

2002-05-15 music swapping copyright intellectual property music piracy bankruptcy purchase

ownership

NewsScan

#### NAPSTER PONDERS BANKRUPTCY

Napster is considering filing for Chapter 7 bankruptcy protection following the breakdown of talks with Bertelsmann, which wanted to take a majority stake in the online music swapping business. Bertelsmann was offering between \$15-20 million for the stake, but the board was split between John Fanning, uncle of Napster founder Shawn Fanning, and former Napster CEO Hank Barry and John Hummer of Hummer Winblad Venture Partners. At the same time, Napster CEO Konrad Hilbers, Shawn Fanning, who serves as chief technology officer, and four other vice presidents announced their resignations. Bertelsmann may still be able to lay claim to Napster's technology, which was used as collateral for the \$85 million in loans it has already made to the company. The failure of Napster would signal a major victory for the entertainment industry in the battle for control over digital music and film, but some Silicon Valley groups warn such a view may be short-sighted: "Hollywood needs to offer a legal and suitable legitimate opportunity for downloading movies," said Intel chairman Andy Grove. "It is self-protection. But technology always wins in the end." (Financial Times 15 May 2002) http://news.ft.com/news/industries/internet&e-commerce

### BERTELSMANN BUYS NAPSTER'S ASSETS FOR A SONG

Bertelsmann is acquiring Napster's brand and products for \$8 million and will forgive \$85 million in loans it has already made to the online music swapping service, which is in the process of filing for Chapter 11 bankruptcy protection. The announcement came as a surprise, because negotiations over a possible sale had broken down last week -- at that point, Bertelsmann was offering \$15-20 million for the company. Under the new deal, Konrad Hilbers and Shawn Fanning, who had resigned last week, will rejoin, with Hilbers assuming the position of chairman in addition to his earlier role as CEO, and Fanning re-assuming his title of chief technology officer. Bertelsmann hopes to relaunch Napster as a paid service. It is already a backer of MusicNet, which it operates in combination with AOL Time Warner and EMI Group, and sources close to the company say it has not yet decided how it will position the two separate online music ventures. (Financial Times 17 May 2002) http://news.ft.com/news/industries/media

Category 19.2 Music piracy

2002-05-28 intellectual property copyright music piracy lawsuit

FindLaw Download This 87

## MUSIC INDUSTRY TAKES SONG-SWAPPING SITE TO COURT

In its latest attempt to halt music piracy, a contingency of music industry groups, including the labels, songwriters and music publishers, filed a lawsuit against American file-sharing Internet service Audiogalaxy.com. The Recording Industry Association of America (RIAA), a powerful trade association for the music labels, and the National Music Publishers Association (NMPA), filed the suit on Friday in a New York federal court.

http://news.findlaw.com/entertainment/s/20020528/medialawsuitdc.html

View the Complaint (ZOMBA RECORDING, CORP. v. AUDIOGALAXY, INC.)

http://news.findlaw.com/hdocs/docs/recordcos/zmbaudglxy52402cmp.pdf

Category 19.2 Music piracy

2002-06-19 P2P peer-to-peer network file sharing permission settlement copyrght intellectual

property music piracy

### Edupage

#### AUDIOGALAXY TO SEEK PERMISSION FOR SWAPS

Audiogalaxy agreed to obtain permission from a songwriter, music publisher, or recording company to use and share copyrighted music before allowing people to swap copyrighted songs using its file-trading service. The concession was part of an out-of-court settlement with the Recording Industry Association of America, National Music Publisher's Association, and Harry Fox Agency, which sued the company a year after Audiogalaxy began filtering copyrighted music from its system. The plaintiffs claimed that the filters failed to perform adequately. Audiogalaxy also agreed to pay an undisclosed sum to settle the suit. It remains to be seen whether the company can survive without the free music services it offered previously. Napster, which shut down after its filters failed to perform adequately, has not resumed service. CNET, 18 June 2002 http://news.com.com/2100-1023-936932.html

Category 19.2 Music piracy

2002-06-19 P2P peer-to-peer networks search engines bots investigation intellectual property

movies films piracy

#### Edupage

#### SOFTWARE SEARCHES FOR ILLEGAL MOVIES

A software program called Ranger searches Web sites, chat rooms, newsgroups, and peer-to-peer file-sharing sites for illegal movies on behalf of film studios represented by the Motion Picture Association of America. Ranger covers 60 countries, searching in English, Chinese, and Korean for pirate movie sites. Some of its targets object to the software's findings, however. Internetmovies.com has filed suit against the MPAA because Ranger identified its Web site as a movie pirate in 2001, prompting the company's Internet service provider to stop access.

Washington Post, 18 June 2002

http://www.washingtonpost.com/wp-dyn/articles/A5144-2002Jun18.html

Category 19.2 Music piracy

2002-06-21 music piracy file-swapping network copyright intellectual property patent law court

bankruptcy assets licenses

# Edupage

## NAPSTER TECHNOLOGY OWNERSHIP CHALLENGED

PlayMedia Systems claims that it provided key parts of the Napster technology, which cannot, therefore, automatically be transferred to Bertelsmann in its purchase of Napster's assets. PlayMedia created the MP3-playing functions of Napster's original file-swapping software and security features of the planned subscription service. PlayMedia representatives said that the company does not plan to interfere with the bankruptcy proceedings and sale of assets to Bertelsmann, but wants to protect its technology licenses during those proceedings.

CNET, 19 June 2002

http://news.com.com/2100-1023-937459.html

Category 19.2 Music piracy

2002-06-28 P2P peer-to-peer music piracy countermeasures intellectual property copyright

violations information warfare theft spoofing denial-of-service attack swamping corruption

## NewsScan

## MUSIC INDUSTRY WAGES GUERRILLA WARFARE AGAINST P2P SERVICES

In a practice called "spoofing," the music industry has been swamping online music-swapping services like Morpheus, Kazaa, and Grokster with thousands of phony or mangled music files rather than the sought-after songs. One music executive, speaking anonymously, says: "We're not using any of this with any kind of promotion or marketing in mind. We're doing this simply because we believe people are stealing our stuff and we want to stymie the stealing." And Cary Sherman, president of the Recording Industry Association of America, says: "From the outset, it's been very clear that one of the only ways -- as a practical matter -- to deal with the peer-to-peer problem is by means of technological measures. There are certainly mechanisms that are available -- that are completely lawful, such as spoofing." (San Jose Mercury-News 27 Jun 2002) http://www.siliconvalley.com/mld/siliconvalley/3560365

Category 19.2 Music piracy

2002-07-03 intellectual property lawsuit prosecution peer-to-peer swapping P2P

NewsScan

#### MUSIC LABELS PLAN ACTION AGAINST INDIVIDUAL SONG-SWAPPERS

The major music labels, working through the Recording Industry Association of America, are preparing to file copyright lawsuits targeting high-volume song providers on peer-to-peer music services. The suits will be part of a broader effort, including a PR campaign that may feature prominent artists urging fans to respect copyright laws. The industry's new legal tack is a marked shift from earlier efforts, which had focused on putting peer-to-peer music services such as Napster, Morpheus and Kazaa out of business. People close to the situation say the RIAA is still in the early stages of planning its efforts and hasn't decided yet exactly what actions should trigger such a lawsuit, although it's agreed that legal retaliation would focus on individuals who supply the largest amounts of music, as well as so-called "supernodes," or people who provide the centralized directories that enable online music-sharing. Suits against individual Internet users could cause a backlash from some fans, but record companies say they have no choice as they face diminishing music sales while home CD-burning has soared. (Wall Street Journal 3 Jul 2002)

http://online.wsj.com/article/0,,SB1025639431553502280.... (sub req'd)

Category 19.2 Music piracy

2002-08-22 intellectual property ISP Internet service provider international jurisdiction music

piracy lawsuit

NewsScan

#### RECORD LABELS SUE ISPs OVER CHINA-BASED SITE

The world's major record labels have sued the major U.S. Internet service and network providers, alleging that their routing systems enable users to access the China-based Listen4ever.com Web site, which provides access to downloadable music from a central location containing thousands of files. The suit alleges that Listen4ever uses offshore servers located in China to host the site where the illegal copying occurs, but that the site uses a U.S. domain name, is written entirely in English, and appears to target an American audience by focusing on U.S. works by artists such as Bruce Springsteen, Red Hot Chili Peppers, Eric Clapton and Whitney Houston. Plaintiffs include units of Vivendi Universal, Sony, Bertelsmann and AOL Time Warner. Defendants in the suit are AT&T Broadband, Cable & Wireless USA, Sprint, Advanced Network Services and UUNet Technologies. (Reuters 17 Aug 2002)

## MUSIC PIRACY SITE IN CHINA SHUTS DOWN

The Recording Industry Association of America and 13 record companies have dropped a lawsuit against four Internet service and network providers they'd sued for providing services to Listen4ever.com, a Chinese Web site accused of distributing pirated music. Apparently Listen4ever.com has ceased operation, making the suit unnecessary unless its owners resume activity under a new name or location. The defendants in the lawsuit were AT&T Broadband, Cable & Wireless, Sprint, and WorldCom's UUNet. (AP/USA Today 22 Aug 2002)

Category 19.2 Music piracy

2002-09-05 music piracy peer-to-peer networking downloads copyright intellectual property

alternative distribution lawsuits trademark infringement

NewsScan

# PRESSPLAY DEBUTS, AIMSTER RESURFACES AS MADSTER [23 Jan 2002]

Pressplay, the online music distribution service backed by Sony and Vivendi Universal, announced its launch this week following about a month of public testing. U.S.-based subscribers will be able to receive up to 300 streamed tunes on demand, as well as up to 30 downloads each month for \$9.95. Heavy users can opt for a \$24.95 deal that provides 1,000 songs and 100 downloads. Unlike rival MusicNet, pressplay subscribers will be able to burn a limited number of songs onto their own CDs. Meanwhile, renegade music-downloading Web site Aimster has resurfaced under a new moniker -- Madster, named after company founder John Deep's daughter Madeleine. Aimster had been under siege by AOL Time Warner, which that the "Aimster" name and Internet domain infringed on its trademarked AIM instant messaging software. (Newsbytes 23 Jan 2002) http://www.newsbytes.com/news/02/173858.html

## INJUNCTION AGAINST MADSTER

A U.S. district court in Chicago has ruled in favor of the record companies and the Recording Industry Association of America, which had sued the file-sharing company Madster over the use of its file-swapping services by individuals who misappropriated copyrighted music. The said Madster?s very reason for being seemed to be "the facilitation of and contribution to copyright infringement on a massive scale." Madster founder Johnny Deep says his company has no way of knowing how people are using the service, since the files are all encrypted. More to come. (AP/San Jose MercuryNews4 Sep 2002) http://www.siliconvalley.com/mld/siliconvalley/4003605

Category 19.2 Music piracy

2002-09-26 intellectual property music download e-commerce

NewsScan

#### ALBUM LAUNCHES IN STORES AND ON THE WEB SIMULTANEOUSLY

Music artist Peter Gabriel is exploring ways to incorporate legitimate music downloading into the distribution strategy for his latest album, "Up." On Tuesday, at the same time CDs were arriving at music stores to be sold, the album was also available online as a hi-fidelity download embellished with several security features to prevent unauthorized sharing. The online album is priced at \$9.99 while the CD version carries a list price of \$18.98. The downloaded version can be transferred to digital audio players supporting Microsoft's Windows Media Audio format and can also be burned up to two times on blank CDs. While some popular singles have been offered for sale online in the recent past, Gabriel's is the first full-length release from a major artist. (AP 26 Sep 2002)

http://apnews.excite.com/article/20020926/D7M9GBP82.htm

Category 19.2 Music piracy

2002-11-27 intellectual property music copyright violations theft piracy

NewsScan

#### FIGHT AGAINST INTERNET FILE-SWAPPING CALLED HOPELESS

Four Microsoft researchers (speaking only for themselves) have told an ACM workshop that the attempt to stop people from using digital file-swapping services is entirely futile; they believe that the technology is moving too fast to be stopped, and explain that previous services (such as Napster) could be forced out of business only because relatively few people provided most of the material. In contrast, the newer services such as Kazaa are attracting too many contributors to keep a rein on. The researchers (Peter Biddle, Paul England, Marcus Peinado, and Bryan Willman) argue that the only way the music and video industries can compete with Kazaa and similar services is to make music and video products much less expensive and much easier to obtain. (BBC 27 Nov 2002)

http://news.bbc.co.uk/1/hi/technology/2502399.stm

Category 19.2 Music piracy

2002-12-04 intellectual property piracy legal action international lawsuits threats privacy ISP

Internet service providers

NewsScan

#### DANISH ANTI-PIRACY GROUPS SENDS BILLS TO VIOLATORS

The Copenhagen-based AntiPiratGruppen, an organization whose efforts to stop theft of digital media are supported by the Danish entertainment industry, has found a new strategy. Instead of attacking Internet service providers for allowing copyright violations to happen, the organization goes directly against the violators themselves, sending them bills ranging from \$130 to \$13,300. (The \$13,300 bill went to a disc jockey). If the recipients of bills do not pay up they will be sued. Various Danish newspapers and consumer groups are upset that Internet service providers have cooperated with AntiPiratGruppen by helping it identify copyright violators. (AP/USA Today 4 Dec2002)

http://www.usatoday.com/tech/news/techpolicy/2002-12-03-music-swap\_x.htm

Category 19.2 Music piracy

2002-12-04 intellectual property piracy legal action injunction file-sharing music

NewsScan

# JUDGE ORDERS MADSTER TO SHUT DOWN

A federal judge in Chicago has issued a temporary restraining order against Madster, telling it to immediately disable its file-servers. U.S. District Judge Marvin Aspen said that record labels "will continue to suffer irreparable harm" otherwise. The Madster Web site continued to advertise \$4.95 a month memberships last night, although downloads of the company's file-sharing software were not available. Lawsuits against Madster (formerly Aimster) had been on hold following its March bankruptcy filing, but a bankruptcy judge recently lifted the stay for the purpose of allowing plaintiffs to seek a preliminary injunction motion. That motion was issued October 30, but the service disregarded the order, which set the stage for yesterday's restraining order. The order is in effect through December 22, barring further notice from the court. (AP 4 Dec 2002)

http://apnews.excite.com/article/20021204/D7NMPD1G0.html

# 19.3 Movies / TV piracy

Category 19.3 Movies / TV piracy

2002-02-06 video online distribution copyright alternative

NewsScan

#### VIVENDI PLANS ONLINE VIDEO SERVICE

Vivendi Universal is launching MP4.com -- a Web site that features a collection of short videos, including animated flicks, feature film-related content, movie trailers and games -- in a few weeks. MP4.com piggybacks on the concept of MP3.com, a music-aggregation site that Vivendi acquired last May. The move into online video follows Sony's debut last September of Screenblast, a site that offers would-be film and animation makers the publishing tools to create video, animation and music. The target user group is 18- to 24-year-olds, an age cohort most likely to have access to broadband connections in dorms or on college campuses. "The concept of MP4 is good if Vivendi can afford the bandwidth and the streaming costs that could attract a big audience," says a digital media researcher at Raymond James Financial. In recent years, a number of similar endeavors have failed to find a viable business model, with Pop.com, AOL Time Warner's Entertaindom, Digital Entertainment Network, Pseudo Programs, CMGI's iCast, and Icebox all falling victim to the dot-com debacle. (CNet News.com 6 Feb 2002)

http://news.com.com/2100-1023-831091.html

Category 19.3 Movies / TV piracy

2002-02-20 video online distribution copyright alternative

NewsScan

#### MGM AND CINEMANOW PLAN VIDEO-ON-DEMAND OVER THE NET

MGM is teaming up with CinemaNow of Marina del Rey, Calif., to become the first major Hollywood studio to offer video-on-demand via the Internet. The companies will offer both downloadable and "streamed" versions of "What's the Worst That Could Happen?" and "The Man in the Iron Mask" to any consumer with a high-speed Internet connection and a Windows-based computer. "Our intention in the next two years is to find out as much as we can about how consumers want VOD delivered, what they think about it, [and] how much they want to pay," says MGM Home Entertainment marketing VP Blake Thomas. MGM had previously joined with four other Hollywood studios in the "Movielink" joint venture, but that effort and its rival, Movies.com, have become bogged down in an antitrust probe by the Justice Department. The MGM movies will be available at two streaming speeds: 300 kbps, which is described as a near-VHS-quality picture, and 700 kbps, which is between VHS and DVD quality. Prices will range from \$2.99 to \$5.99, depending on location and Internet connection. (Los Angeles Times 20 Feb 2002)

http://www.latimes.com/technology/la-000012921feb20.story?coll=la%2Dheadlines%2Dtechnology

Category 19.3 Movies / TV piracy

2002-09-09 online video movies distribution e-commerce intellectual property piracy

NewsScan

#### VIDEO-ON-DEMAND GETS A BOOST

Two major deals announced today signal the first steps toward building a marketplace for online films: Movielink, the digital-film venture backed by five major Hollywood studios, has struck an agreement with IBM to provide the servers that will host its movies, and CinemaNow, a rival VOD majority owned by Lions Gate Entertainment, signed its first major-studio licensing deal with Warner Bros., allowing it to offer "dozens" of its titles, including the blockbuster "Harry Potter and the Sorcerer's Stone." CinemaNow, which is already operational, says it's negotiating with other studios to secure film licenses, and Movielink CEO Jim Ramo says his venture is "moving forward with all the necessary ingredients for launch in a timely manner." (Wall Street Journal 9 Sep 2002)

Category 19.3 Movies / TV piracy

2002-10-30 DVD copyright intellectual property backup copies piracy movies

NewsScan

# 'WE FEEL IT'S LEGAL': NEW DVD BACKUP SYSTEM

The software developer 321 Studios, based in St. Louis, Mo., plans to start using its Web site to sell downloadable copies of its software for making backup copies of DVD movies. The Motion Picture Association of America (whose chairman Jack Valenti has called DVD recorders "the newest incarnation of movie piracy") will probably file a lawsuit against 321, but the company's president says: "Our position is that our product is for the purpose of making backup copies of the movies you already own. We feel it's legal." (USA Today 29 Oct 2002)

Category 19.3 Movies / TV piracy

2002-12-11 DVD movie counterfeits piracy copyright infringement intellectual property lawsuits

NewsScan

# HOLLYWOOD AND THE PIRATES

The Motion Picture Association of America (MPAA) has filed copyright-infringement lawsuits against individuals in eight states it accuses of using the Internet to sell bootlegged DVD copies of movies. The MPAA detected the piracy by purchasing some of the DVDs and then examining the contents. (AP/USA Today 11 Dec 2002)

# 19.6 Counterfeit currency, credit-cards, other negotiable tokens

Category 19.6 Counterfeit currency, credit-cards, other negotiable tokens 2002-01-10 credit-card fraud clone counterfeit hack

RISKS 21 86

David Farber wrote in RISKS:

>Homemade machines costing about \$50 are being used to read credit-card mag-stripes, without having to steal the cards. The information is then e-mailed abroad, where cloned cards are fabricated. This has become a billion-dollar-a-year enterprise.

# 19.7 Counterfeit legal or business documents

Category 19.7 Counterfeit legal or business documents

2002-03-22 intellectual property rights SLAPP strategic lawsuit against public participation free

speech copyright infringement search engine

#### NewsScan

#### GOOGLE PULLS, THEN RESTORES, LINK TO ANTI-SCIENTOLOGY SITE

Caught between the Church of Scientology (which says it was protecting its own copyrighted material) and the Electronic Frontier Foundation (which says it was protecting free speech), the Google search service first removed, then replaced, reference to a site critical of Scientology. The Church of Scientology has accused the site Xenu.net of "wholesale, verbatim copyright infringement" for posting large quantities of copyrighted material; Xenu and the Electronic Frontier Foundation have charged that the Church was using copyright laws to stifle criticism. (Reuters/San Jose Mercury News 21 Mar 2002) http://www.siliconvalley.com/mld/siliconvalley/2910195.htm

Category 19.7 Counterfeit legal or business documents

2002-03-29 counterfeit confidentiality identity theft forgery fraud

RISKS 22 02

Someone has been circulating a fraudulent "W-9095" form claiming to be from the US Internatl Revenue Service (IRS). The counterfeit form, entitled, "Application Form For Certificate Status/Ownership For Withholding Tax," asks for all kinds of detailed information perfect for perpetrating identity theft. The fraud was discovered when a potential victim brought it in to a bank for clarification.

# 19.8 Plagiarism

Category 19.8 Plagiarism

2002-08-08 plagiarism intellectual property professors students essays

NewsScan

ANTIPLAGIARISM SOFTWARRE: 'WHOSE ESSAY IS IT', ANYWAY?'

Various academic institutions now use antiplagiarism software to catch student cheaters -- but some critics say such software tramples on student rights, specifically their copyrights. Example: the antiplagiarism product Turnitin.com expands its database by keeping copies of scanned student papers without getting the permission from the student; the papers can then be used for comparison with new submissions as they are received in the future. Is this a permissible practice? Sure, says Turnitin -- this use of the papers doesn't threaten any potential commercial value of the papers and is well within "Fair Use" rules. [Antiplagiarism aficionados will enjoy Bernard Malamud's 1961 novel "A New Life," in which faculty members work frantically but unsuccessfully to expose a student.] (IEEE Computer Aug 2002)

# 19.9 Counterfeit products (hardware, clothing etc.)

Category 19.9

Counterfeit products (hardware, clothing etc.)

2002-04-14

data integrity authenticity illusion virtual reality fraud pretence simulation VR

NewsScan

#### VIRTUAL NEWS SETS

More than 40 U.S. television stations and many production studios are now using virtual newsrooms that give the impression that newscasters are broadcasting from gigantic, futuristic sets when the truth is that they are actually in cramped, narrow rooms. How is it done? Just about everything in the room is painted a certain shade of blue, and when the TV camera records that particular color it substitutes digital imagery to make people and any objects not in that color appear superimposed on the digital set. So when you see a news anchor standing in front of a huge wall of video monitors, you're just seeing "smoke and mirrors" (or maybe just mirrors -- unless the anchor's excitement set his pants on fire). (New York Times 14 Mar 2002) http://www.nytimes.com/2002/03/14/technology/circuits/14HOWW.html

# 1A3 Biographical notes on individual criminals

Category 1A3 Biographical notes on individual criminals

2002-03-04 criminal hacker virus writer subculture personality teenager adolescent rebellion

reputation woman girl female stereotype e-mail enabled worm

#### NewsScan

#### GIRLS JUST WANT TO HAVE HACKER FUN [4 Mar 2002]

An unidentified hacker who claims to be a 17-year-old girl says she was motivated to write the "Sharpei" worm to dispel the notion that there aren't any female virus writers and to annoy Microsoft, rather than to have it spread to actual computer users. Going by the name "Gigabyte," she says on her Web site that she's a high-school senior who takes kick-boxing classes and likes techno and trance music. A consultant for Sophos, the U.K. based security company that reported the worm says, "I just don't know what she's accomplishing by this. She's neither hurting nor helping people." The worm was written to spread via Outlook Express e-mail, with a subject line reading, "Important: Windows Update." (Reuters/New York Times 4 Mar 2002)

http://www.nytimes.com/reuters/technology/tech-tech-feminist.html

Category 1A3 Biographical notes on individual criminals

2002-05-02 virus writer prosecution judgement sentence jail prison fine

NewsScan

### MELISSA VIRUS WRITER NETS JAIL TIME

David L. Smith, creator of the "Melissa" virus, was sentenced Wednesday to 20 months in prison and a \$5,000 fine for his role in unleashing the destructive program that caused more than \$80 million worth of damage worldwide in 1999. Smith, who is among the first people ever prosecuted for creating a computer virus, called the act a "colossal mistake." "My curiosity got the better of me, as I soon began to write the 'Melissa Virus," he wrote in a letter to U.S. District Judge Joseph A Greenaway Jr. "It didn't take me too long as I borrowed a lot of the code from other viruses that I found on the Internet." Smith could have received up to five years in prison, but prosecutors suggested the shorter sentence, saying he had given authorities extensive assistance in thwarting other virus creators. (AP 1 May 2002) http://apnews.excite.com/article/20020501/D7J85S3O0.html

Category 1A3 Biographical notes on individual criminals

2002-08-06 worm prosecution charge court Trojan

C | Net News http://news.com.com/2100-1001-948596.html

In August 2002, five Israeli teenagers from grades 8, 10 and 11 were charged in Haifa with creating the Goner worm (aka Pentagone and Gone), a trivial piece of work that disabled some firewalls and antivirus tools and spread through ICQ and email. The worm did cause some servers to crash at various organizations around the world including NASA computer centers.

# 1A6 Criminal hacker psychology

Category 1A6 Criminal hacker psychology

2002-03-05 criminal hacker psychology worm social engineering

NewsScan

#### GIRLS JUST WANT TO HAVE HACKER FUN

An unidentified hacker who claims to be a 17-year-old girl says she was motivated to write the "Sharpei" worm to dispel the notion that there aren't any female virus writers and to annoy Microsoft, rather than to have it spread to actual computer users. Going by the name "Gigabyte," she says on her Web site that she's a high-school senior who takes kick-boxing classes and likes techno and trance music. A consultant for Sophos, the U.K. based security company that reported the worm says, "I just don't know what she's accomplishing by this. She's neither hurting nor helping people." The worm was written to spread via Outlook Express e-mail, with a subject line reading, "Important: Windows Update." (Reuters/New York Times 4 Mar 2002) http://www.nytimes.com/reuters/technology/tech-tech-feminist.html

# 1B1 Adult pornography

Category 1B1 Adult pornography

2002-05-06 online pornography gambling

NewsScan

#### INTERNET FINDS NEW WAY TO LOSE MONEY: ONLINE PORNOGRAPHY

Oh, the trials of the pornographer. How do you stand out against all the competition? With so much porn available for free, how do you get people to pay? With broadband connections widely available, how do you prevent customers from downloading everything quickly and then canceling their subscriptions? The days of easy profit on the Web are over, even for pornographers. The marketing and publicity for one well-known sex site says, "I think things are shaking out. The same rules have always applied to this business as any other." Another problem for online pornographers is that credit card companies tend to view them as "slow-pays" or deadbeats, and consider them to be a major source of fraud complaints and illegal activities such as underage sex and bestiality. So what's a poor pornographer to do? Many of them are now turning to online gambling. They're not really interested in sex, they're interested (surprise) in money. (San Jose Mercury News 4 May 2002) http://www.siliconvalley.com/mld/siliconvalley/3200456.htm

Category 1B1 Adult pornography

2002-05-08 youth children pornography report research sexual predators online

RISKS, http://bob.nap.edu/html/youth\_internet/

22 06

[T]he National Academies' report entitled "Youth, Pornography and the Internet" was released on May 2. The report examines approaches to protecting children and teens from Internet pornography, threats from sexual predators operating on-line, and other inappropriate material on the Internet. It discusses social and educational strategies, technological tools, and policy options for how to teach children to make safe and appropriate decisions about what they see and experience on the Internet. Chaired by former Attorney General Dick Thornburgh, it's the most comprehensive study yet on the topic.

More information on the report is available at:

http://www4.nationalacademies.org/onpi/webextra.nsf/web/porn?OpenDocument

The report itself is available online at:

http://bob.nap.edu/html/youth\_internet/

Category 1B1 Adult pornography

2002-08-16 online pornography mainstream providers

NewsScan

#### REALNETWORKS MULLING ADULT PAY-PER-VIEW

RealNetworks has made no secret of its desire to emulate the cable industry, with its core business strategy focused on delivering name-brand content and software services to paying customers. The company is currently in discussions with several audio and video producers to expand the lineup on its RealOne SuperPass service, and VP Dave Richards says that although there are no immediate plans to offer adult-only fare, the possibility of a future venture cannot be ruled out. "We expect we will have different tiers" of service. "Maybe even an adult tier." And while some analysts say getting into porn distribution is the kiss of death for mainstream publishers, others point out that the cable industry has dabbled in adult content for years without sparking a major backlash. Still, several Internet companies have tested the waters in the booming online pornography industry and decided to pull back. In April 2001, Yahoo yanked all pornographic ads, auction items and merchandise from its site in response to consumer complaints, and in January 2000, Ask Jeeves shelved plans to launch a separate search engine for pornography in order to preserve its family-friendly image. (CNet News.com 15 Aug 2002) http://news.com.com/2100-1023-950053.html?tag=fd\_top

Category 1B1 Adult pornography

2002-08-29 online pornography national archives

NewsScan

#### AUSTRALIA'S NATIONAL LIBRARY TO ARCHIVE INTERNET PORN

Australia's National Library is breaking new ground in digital archiving -- as part of its six-year-old project to record a selection of Web sites for historical purposes, the Library now says it will include a smattering of Internet pornography. "Whether we like it or not, pornographic sites are part of the Australian Web and we feel it is necessary to collect a sample, a small sample, of sites that reflect the use of some Australians of that kind of site," said Margaret Phillips, manager of the Library's online collection, in an interview with the Australian Broadcasting Corp. When asked whether she anticipates a backlash from those who feel such images have no place in the National Library, Phillips replied: "There may be a backlash, we haven't been expecting it. From time to time there is criticism of the kind of material the Library collects, both in print and online. But it is not the role of the National Library to act as the role of the censor." (ABC Online 27 Aug 2002) http://www.abc.net.au/am/s659750.htm

Category 1B1 Adult pornography

2002-09-13 pornography online commercial e-commerce auction bids

NewsScan

#### SPANISH PORN COMPANY BIDS ON NAPSTER TRADEMARK

Private Media Group, a Spanish adult-entertainment company, has made an all-stock offer worth \$2.4 million in a bid to acquire the trademark and Web address of the now-defunct Napster. Last week, a bankruptcy judge rejected a \$9 million bid by Bertelsmann, saying the deal wasn't negotiated at arm's length, as required by law. Private Media said it plans to use the Napster trademark to promote its collection of "top quality" adult-oriented fare at a reasonable price, and to offer adults the ability to swap adult content for free. Private Media owns the global copyrights to what it claims is the largest library of adult-oriented content in the world. "Acquiring Napster is our way of entering the peer-to-peer marketplace for adult content in a closed environment," says Private Media CEO Charles Prast. "Along with Hollywood and the recording industry, we have become increasingly concerned about the level of copyright infringement inherent in the peer-to-peer file swapping services." (Reuters/CNet 12 Sep 2002)

http://news.com.com/2100-1023-957784.html?tag=fd\_top

#### ROXIO WINS BID FOR NAPSTER

Roxio, the top seller of CD-burning software, has successfully bid to acquire Napster's technology, the Napster.com domain name, and the Napster brand for \$5 million in cash and warrants to buy 100,000 shares of Roxio stock. The move took some music execs by surprise, but Roxio CEO Chris Gorog hastened to reassure the record labels that he planned to promote legitimate use of Napster. "Based on my relationships and general discussions with the labels, I think they will be excited at this announcement. They know that anything that Roxio will do in this space will be respectful of artist rights and will be working toward a commercial solution." (Los Angeles Times 15 Nov 2002)

Category 1B1 Adult pornography

2002-10-16 video games pornography children adolescents teens parents

NewsScan

#### HOLIDAY VIDEO GAMES ARE RISQUÉ BUSINESS

This holiday season will serve up some of the raciest footage yet on the upcoming releases of new computer and video console games. The offerings range from "Dead or Alive Xtreme Beach Volleyball," which offers buxom, scantily-clad volleyball players who "jiggle" realistically, to "BMX XXX," in which players rack up cash on the circuit and then get to spend it at a local strip joint, watching live-action footage of topless dancers. The BMX game also allows players to design their own topless biker characters, starting with chest measurements. "Consumers seem to be getting a little bored of a guy on a bike on a ramp," says Ben Fischbach, brand manager for Acclaim. "This product is a true comedic entertainment property. We really look at this game as 'American Pie' meets 'Airplane' meets 'Howard Stern." And while BMX XXX is rated "M" for players 17 and up, there are a number of other BMX games on the market now aimed at younger players, and the Parents Television Council worries that parents might grab it off the shelf without noticing the rating. In an effort to alert parents to the mature content, PTC has issued a warning about the game: "This may look like an ordinary biking game but it is the first sports game to carry an M rating and feature strippers, public urination, and yes? dog humping," reads the notice. (CNN/Money 17 Sep 2002)

#### VIDEO SEXXX GAMES

Video games are getting sexier and sexier. Industry analyst Michael Pachter says that sales of M-rated games (so-called "Mature" games) in the U.S. are expected to double this year from 7% overall to 14%, thanks to titles such as "BMX XXX," "The Getaway," and "Grand Teft Auto: Vice City," the last of which features interactive prostitutes whose services players can buy to boost their "health points." (Los Angeles Times 10 Oct 2002) http://makeashorterlink.com/?U23112112

## MAJOR RETAILERS WON'T SELL "ADULT" VIDEO GAMES

National retailers Wal-Mart, Toys R Us, and KB Toys have decided not to carry a new video game -- BMX XXX -- that features full-action nudity, prostitutes, and pimps, and is described by its creators as "a game of cultural sophistication and artistic aspiration." Wal-Mart executive Tom Williams says, "We're not going to carry any software with any vulgarity or nudity -- we're just not going to do it." The chief executive of Acclaim Entertainment, the company that distributes the game, defends it as a spoof and says: "What we're doing here is funny." (Reuters/USA Today 16 Oct 2002)

# 1B2 Child pornography

Category 1B2 Child pornography

2002-07-10 child pornography investigation arrests

NewsScan

#### FBI ARRESTS 10 IN INTERNET CHILD PORN INVESTIGATION

Among those in Manhattan and Brooklyn arrested by the FBI yesterday in its ongoing "Operation Candyman" investigation of Internet child pornography were a U.S. Army sergeant, two former NYC police officers, a subway conductor, a construction company owner, and a retired firefighter. If convicted, they will face up to five years in a federal prison. A government official said: "As you can see, those who collect and receive images of sexual abuse of children are not nameless faces lurking in cyberspace, nor are they shadowy figures leering in a dark alley. But they come from every cross-section of our society and both our urban and suburban neighborhoods." The porn site made available to its members images of real children 12 and under having sex with adults. (New York Times 10 Jul 2002) http://partners.nytimes.com/2002/07/10/nyregion/10PORN

Category 1B2 Child pornography

2002-12-02 virtual move characters child pornography

NewsScan

## MOTION-CAPTURE TECHNOLOGY REWRITES THE SCRIPT

Robert Zemeckis's new film project, "The Polar Express," is pushing the envelope in film-making technology, creating a live-action movie without filming any true "live" action. All of the scenes will be shot with a digital camera in front of a blank screen, with the sets to be filled in later by computers. The actors will be wired with motion-capture sensors that will store each movement digitally, to be used later as a guide for the animators who will create the actual film footage. Unlike other digitally animated movies like "Shrek," "The Polar Express" animators are striving to create images that actually look like the actors who will "star" in the film. The film will also combine characters based on real and virtual people -- for instance, the child version of Tom Hanks' character will be backward engineered using photos of Hanks as a youth and 3D digital representations of his current facial and muscle structure. "This is an ambitious, exciting project for us. We've seen the early tests, and it's like nothing I've ever seen," says Martin Shafer, chairman and CEO of Castle Rock Entertainment, which is making the movie. (Los Angeles Times 2 Dec 2002)

# 1B3 Pedophilia, kidnapping, Net-adoption fraud

Category 1B3 Pedophilia, kidnapping, Net-adoption fraud

2002-10-31 Web logs blogs children hysteria evidence

NewsScan

#### CHILD SAFETY ON THE WEB

The Internet personal diaries known as Blogs (or, more formally, Web logs) are providing the latest source of concern to parents and educators worried about the safety of children on the Net; author Jean Amour Polly says: "The Internet has moved on into new territory. Strangers can comment on the diaries and even e-mail kids advice and comfort." But criminologist David Finkelhor, who studies Internet crime and teaches at the University of New Hampshire, warns against hysteria on the subject: "There are new perils for kids, but no evidence that kids are on the whole more endangered today as a result of the Internet. There's no sign of an incredible tidal wave of mayhem and danger that's washed onto our shores." (New York Times 31 Oct 2002)

# 1B4 Stalking & harassment

Category 1B4 Stalking & harassment

2002-03-12 online culture pornography children chat spam cybersex relations parental

supervision

#### NewsScan

#### 30% OF TEENAGE GIRLS SUFFER ONLINE HARASSMENT

Thirty percent of teenage girls have been sexually harassed in a chat room, according to a poll conducted by the Girl Scout Research Institute. Only 7% had reported the harassment to their parents, however, because they feared being banned from online activities. Most of the girls said they tried to avoid pornographic sites, but that they sometimes ended up there by accident. They also reported receiving a lot of pornographic spam. And while the GSRI said parents should pay more attention to their daughters' online activities, 87% of the girls polled said they could chat online without their parents knowledge and 54% said they could conduct a clandestine cyber relationship. (NUA Internet Surveys 11 Mar 2002) http://www.nua.com/surveys/?f=VS&art\_id=905357736&rel=true

Category 1B4 Stalking & harassment

2002-04-15 Internet harassment bullying stalking threats e-mail chat text instant message

culture children violence intimidation

#### NewsScan

#### **BULLYING GOES ONLINE**

Schoolyard bullies are harnessing technology to pursue their victims around the clock, warned UK children's charity NCH, which reports that one in four school children suffer from bullying via text-message, e-mail or in Internet chat-rooms. "The crucial difference from traditional bullying is that in the past kids who are being bullied could go home and find a safe haven," says NCH associate director John Carr. "But if they're bullied on their mobile (phone) or on the Internet, then it's ever-present." Carr said a survey conducted last month showed that one in six children aged 11 to 19 had received bullying text messages and about one in ten had been bullied over the Internet. (Reuters 15 Apr 2002)

http://story.news.yahoo.com/news?tmpl=story&cid=581&ncid=581&e=1&u=/nm/20020415/tc\_nm/britain\_bullying\_dc\_1

# 1B5 Gambling

Category 1B5 Gambling

2002-01-14 online gambling legalization interactive TV handheld

NewsScan

#### COMPANIES GAMBLE ON ONLINE WAGERING

A growing number of companies are developing online gambling technologies, betting that cyberwagering will be legalized in the U.S. in the not-too-distant future. Interactive Systems Worldwide has designed interactive-television gambling software for German media firm Kirch Group that will enable European sports fans to bet from their own living rooms, and Interactive chairman Barry Mindes expects it will be available for this year's soccer World Cup. Interactive Systems is now working on a handheld gambling device and is hoping to introduce an online "contest" concept in the U.S. based on the gambling software. Under current U.S. law, online gambling is prohibited but TV viewers can enter contests to win prizes such as a car. Mindes envisions users answering a list of questions posed by an advertiser to rack up credits that could then be used for playing the game. (Wall Street Journal 14 Jan 2002)

http://interactive.wsj.com/articles/SB1010960972280769280.htm (sub req'd)

Category 1B5 Gambling

2002-01-31 online gambling gaming mobile telephone Internet

NewsScan

#### MOBILE GAMING SET TO BOOM

Almost half of all European mobile phone customers will be using their handsets to play games by 2005, according to a recent Forrester Research report, as users take advantage of snazzy new handsets and upgraded wireless networks. "The increase in wireless bandwidth and better phones will attract more firms to offer mobile games. Just as an increase in Internet-ready PCs pushed more companies to offer Web services, a bigger audience for mobile games will make firms like Eidos Interactive and Electronic Arts follow in the footsteps of Riot Entertainment and Picofun," says the report. As more games become available, the number of mobile game users is anticipated to rise from 5 million currently to 130 million by 2005. And while most of these players will be young, older gamers are expected to join the fun next year as classic 1970s- and '80s-era games, such as Pong, Frogger and Space Invaders, are revamped for the mobile platform. However, in order to capitalize on this new source of revenue, "operators must curb their greed," warns the report, saying that to ensure developers to continue to produce the games, operators must share their revenues with them. Forrester predicts that over the next five years, ad agencies will begin to acquire their own game development groups to create games for advertising and branding purposes. Television and film studios will also jump into the mix, with mobile games based on shows such as "Who Wants to Be a Millionaire?" (ElectricNews 31 Jan 2002)

http://www.electricnews.net/news.html?code=5909714

Category 1B5 Gambling

2002-06-18 credit card online gambling bank block abuse fraud

NewsScan; http://www.nytimes.com/2002/06/15/business/15GAMB.html

90

#### CREDIT CARDS BANNED FOR INTERNET GAMBLING

Citibank has agreed to block use of its credit cards for Internet gambling after New York State regulators said the bank could face criminal prosecution for aiding in the promotion of online gambling, which is illegal in New York. Citibank, with 33 million Visa and MasterCard holders, is the largest credit card issuer in the United States. Citibank also agreed to pay \$400,000 to nonprofit agencies that provide gambling counseling. Other major credit card issuers, including Providian Bank, have already said they will try to block use of their cards for Internet gambling. Like other credit card issuers, Citibank is motivated to block the transactions for additional reasons, such as the "increased potential for fraud loss" and higher "delinquency rates" on the online gambling charges. New York Times, 15 June 2002 (registration req'd)

Category 1B5 Gambling

2002-09-11 online gambling law ruling international Greece casino Internet café

NewsScan

#### GREEK COURT REVERSES BAN ON VIDEO GAMES

The first case to test the new Greek law banning people from playing video games in public places has been thrown out of court, setting the country's legal establishment on a collision course with the state. Legislation passed in July forbade the games as part of a drive to stamp out illegal gambling, but it has been harshly criticized by the Internet community for not making a distinction between gaming and interactive gambling. Under Greek law, gambling is permitted only in licensed casinos, and the draconian legislation was enacted in response to an unlicensed slot-machine scandal that had embarrassed the government. The two Internet café owners charged with violating the ban could have faced jail sentences of up to three months and fines of \$4,950 each, as well as the loss of their business licenses. Greece's Internet Café Owners Union welcomed the ruling, but say that their business has dropped precipitously since the law was passed. Computer usage in Greece is one of the lowest in the European Union, and Internet cafés have been credited with helping to expand access. (BBC News 10 Sep 2002) http://news.bbc.co.uk/1/hi/technology/2249656.stm

Category 1B5 Gambling

2002-10-02 online gambling law bill proposed legislation

NewsScan

#### HOUSE ATTACKS INTERNET GAMBLING

The U.S. House of Representatives has passed a bill that would make it illegal to use credit cards or other forms of electronic payment for gambling on the Internet. Supporters of the legislation see a distinction between casino gambling and offshore gambling. Rep. Joseph Pitt (R-Penn.) says: "It may be impossible to keep illegal gambling sites off the World Wide Web, but it is entirely possible to prevent American credit card companies from completing these transactions that these crooks need to make their money, and that's what this bill does." James Leach (R-Iowa) adds: "Internet gambling serves no legitimate purpose in our society -- it is a danger to the family, it is a danger to society at large." (Austin American Statesman 2 Oct 2002)

Category 1B5 Gambling

2002-10-04 online gambling offshore jurisdiction e-commerce law legislation

NewsScan

#### MGM LAUNCHES ONLINE CASINO

Las Vegas resort operator MGM Mirage has quietly launched an online casino, becoming the first major U.S. gambling company to do so. Its site is open to all for free play, but only residents of the UK, Portugal, Spain, Ireland, South Africa and New Zealand are allowed to open accounts and bet real money. The online casino office is located on the Isle of Man, an island-nation off the coast of Great Britain that has licensed four other Web casinos. The MGM Mirage site uses layers of database-searching software designed to verify that gamblers are who -- and where -- they say they are, and regulators and auditors on the Isle of Man and in London also monitor the network of systems. MGM is hoping that its move will encourage other large casinos to go online, but at the same time, online gambling is running into stiff opposition in Congress, where a bill passed on Tuesday would make it a crime for a gambling business to accept credit cards, checks or fund transfers in connection with unlawful Internet gambling. Gambling industry analysts predict that online casinos are likely to become an established niche in the market, where approximately 1,800 largely offshore Internet gambling sites already generate \$3.5 billion in annual revenues, according to Bear Stearns. (AP/Wall Street Journal 3 Oct 2002)

# 1B6 Auctions

Category 1B6 Auctions

2002-06-11 online auction fraud deception cheat stolen property law enforcement

NewsScan; http://www.siliconvalley.com/mld/siliconvalley/3443962.htm

#### ONLINE AUCTIONS THE NEWEST WAY TO FENCE STOLEN GOODS

Online auctions such as eBay are the newest way to fence stolen property, because they're so anonymous and so simple. A Santa Clara prosecutor says: "There's no need for the pawnbroker. Internet auctions have suddenly become a really easy way to fence stuff." But law enforcement officials agree that eBay is extremely diligent in helping authorities track down criminals, by running sophisticated anti-fraud operations and by helping prosecutors build legal cases. An executive of the National Consumer League reminds us: "As we always say, if the deal is too good to be true, it usually isn't." (San Jose Mercury-News 10 Jun 2002)

Category 1B6 Auctions

2002-12-05 Internet online auction scam fraud indictment

NewsScan

# INTERNET AUCTION SCAM

A 27-year-old Los Angeles man, Chris Chong Kim, has been charged with defrauding eBay buyers on six continents who had purchased computer equipment from him but never received delivery of the products they had purchased. The criminal complaint against Kim details losses of \$453,000 to 26 U.S. customers and to eBay and Bank of America. If convicted, Kim will face a penalty of up to 24 years in prison. (Reuters/USA Today 4 Dec 2002) http://www.usatoday.com/tech/news/2002-12-04-ebay-scam\_x.htm

# 1B7 Hate groups, speech

Category 1B7 Hate groups, speech

2002-07-10 terrorist Internet communicaions Web

NewsScan

#### TERRORIST LIFE, INTERNET-STYLE

In recent months sites like azzam.com, almuhajiroun.com, and qassam.net have been set up for terrorists to "make the Internet our tool," and although service providers frequently shut them down they usually reappear someplace else: al-Qaeda's Arabic site alneda.com has reemerged in the past five weeks on different servers in Malaysia, Texas, and Michigan. Most suspected terrorist sites are written in Arabic, proclaim hatred for the U.S., and call on militant Muslims to kill Americans and attack U.S. interests. But there are exceptions: the Islamic alsaha.com site has posted comments accusing bin Laden of being "a disgrace to our religion" and accusing him of having made "a mockery of everything we believe." Do these terrorists have day jobs? The site azzam.com offers the following advice to those who want to fight "the Jewish-backed American Crusaders" without disrupting their own employee benefits plans: "If you are working, either resign from your job and take a year off or request unpaid leave from your employer. Many large companies offer unpaid leave to their employees for periods ranging from two months to one year. That way you can fulfill your obligation [of jihad] and not have to give up your job." (USA Today 9 Jul 2002)

http://www.usatoday.com/life/cyber/tech/2002/07/10/terr

# 1B9 Non-virus hoaxes, urban myths

Category 1B9 Non-virus hoaxes, urban myths

2002-01-30 securities fraud Web marketing gullibility scam SEC government regulators hoax

lesson

# NewsScan

## SEC PLAYS LITTLE HOAX TO WARN INVESTORS OF WEB SCAMS

The Securities and Exchange Commission is a principal agency behind the hoax site www.mcwhortle.com, which purports to provide testimonials from investment analysts and financial exports for an outfit called McWhortle Enterprises, but which greets visitors with the warning: "If you responded to an investment idea like this... You could get scammed!" (AP/San Jose Mercury News 30 Jan 2002)

http://www.siliconvalley.com/docs/news/svfront/046980.htm

## 1C1 Impersonation

Category 1C1 Impersonation

2002-01-24 spoofing forgery impersonation voting information warfare

RISKS 21 89

Nick Brown wrote about a case of e-mail spoofing that backfired because of a spelling mistake. As he reported in RISKS, "An e-mail was sent from the account of the mayor, telling members of a city commission to vote in favour of a plan to extend a local hypermarket. The official, public policy of the city council and the mayor is to oppose this extension. The mail to one member of the commission bounced, because the recipient's name was incorrectly spelled. An assistant to mayor Fabienne Keller, who has access to her mailbox, noticed the "undeliverable" reply and determined that the mail had been sent at a time when the mayor could not have sent it. The general manager of the hypermarket is under police investigation for illegal entry into a computer system, forgery, use of forged documents, and attempted fraud."

#### [French references:]

http://www.dna.fr/cgi/dna/motk/idxlist\_light?a=art&aaaammjj=200201&num=18041610&m1=keller&m2=mairie&m3=http://www.dna.fr/cgi/dna/motk/idxlist\_light?a=art&aaaammjj=200201&num=19049910&m1=keller&m2=mairie&m3=

Category 1C1 Impersonation

2002-10-03 social engineering psychology deceit impersonation trickery penetration

NewsScan

#### DECEIT, NOT TECHNOLOGY, IS THE REAL MENACE TO SECURITY

Reviewing Kevin Mitnick's new book "The Art of Deception: Controlling the Human Elements of Secrecy," Simson Garfinkel writes in the Christian Science Monitor: "Although some will accuse Mitnick of creating a handbook that teaches crooks how to break into organizations, the truth is that we all need to understand these con games to protect against them. To stress this point, his last two chapters contain policies, procedures and training that companies can implement to further protect themselves. In keeping with his premise that the most damaging security penetrations are the result of deceit - not technical penetration - almost none of Mitnick's suggestions is technical in nature. The most important recommendation is that when somebody contacts you claiming to be from your organization, you need to verify that they are working for your organization no matter whether they are asking for your help, offering to help you, or just trying to be friendly." (Christian Science Monitor 3 Oct 2002)

http://www.csmonitor.com/2002/1003/p15s02-bogn.html

## 1C2 Identity theft

Category 1C2 Identity theft

2002-04-04 IRS tax confidentiality penetration security Web encryption plaintext cleartext

Security Wire Digest 4 26

Sandra Kay Miller reported on the growing identity-theft problem in the US in an article published in the Security Wire Digest. The Federal Trade Commission (FTC) noted that about 400,000 victims experienced identity theft in 2001. Miller pointed out that access to tax forms -- including electronically submitted documents -- is a valuable source of information for identity thieves. She wrote, "Last year, the General Accounting Office reported that during security audits, IRS firewalls on e-filing systems did not effectively restrict external access to network, stored unencrypted e-filed returns on systems, practiced poor password management and had very little intrusion detection capability." In addition, some commercial tax preparers also demonstrate shoddy security, although the leading firms seem to protect their clients' data.

Category 1C2 Identity theft

2002-06-27 identity theft spoofing risk Web design credit card

RISKS; 22 13

http://www.cnn.com/2002/TECH/internet/06/26/identity.theft.ap/index.html

Conrad Heiney, writing in RISKS, identified a poorly-thought-out design for an anti-fraud site on the Web: > [A] nongovernmental organization called CardCops is providing a service in which consumers can check to see if their credit cards have been abused in some way.

The check is done by visiting the website and entering your credit card number.

The RISKS here are bad enough to be humorous. Although CardCops themselves appear to be a legitimate organization (at least at time of press), and do not themselves ask for the expiration date required to complete a transaction, there's no protection against copycat websites whose intent is entirely evil, or telephone scams based on the CardCops publicity. The quality of the data is another obvious minefield.

Category 1C2 Identity theft

2002-08-01 social security number SSN privacy consumer identity theft

NewsScan

#### SIMSON SAYS: STOP TOSSING SOCIAL SECURITY NUMBERS AROUND

Privacy advocates have said, and said, and said again, that companies shouldn't use Social Security numbers as identification numbers or passwords -- yet colleges and banks and all kinds of other companies have turned a deaf ear to that plea, because they've been trying to balance security concerns with customer convenience. But Simson Garfinkel, author of Database Nation (and NewsScan Daily contributor), says: "It is the reason we have an epidemic of identity theft right now. The problem here is that people treat the Social Security number as if it is a secret, when in fact it is not." Would new legislation do any good? Garfinkel says no: "We should accept the fact that the Social Security number is a universal identifier, and we should treat it as a public record. Businesses should not use a Social Security number as a password any more than they should use a name." (USA Today 31 Jul 2002)

## 1C4 Anonymity

Category 1C4

Anonymity

2002-11-22

anonymity Internet surveillance law trace technology identifier research intelligence information

#### NewsScan

#### PENTAGON CONSIDERED PLAN TO END ANONYMOUS NET ACTIVITY

After the head of DARPA, the Defense Advanced Research Projects Agency, wondered why it was not possible after the 9-11 terrorist attacks to trace hostile Internet communications back to the origin, a series of technical discussions were initiated, and those discussions led to a proposal called eDNA: "We envisage that all network and client resources will maintain traces of user eDNA so that the user can be uniquely identified as having visited a Web site, having started a process or having sent a packet. This way, the resources and those who use them form a virtual 'crime scene' that contains evidence about the identity of the users, much the same way as a real crime scene contains DNA traces of people." But the project was argued against by a number of angry participants, such as security consultant Mark Seiden who said: "Before people demand more surveillance information, they should be able to process the information they already have. Almost all of our failures to date have come from our inability to use existing intelligence information." DARPA has decided to discontinue funding of the project, and explained that it had been "intrigued by the difficult computing science research involved in creating network capabilities that would provide the same levels of responsibility and accountability in cyberspace as now exist in the physical world." (New York Times 22 Nov 2002)

http://www.nytimes.com/2002/11/22/politics/22TRAC.html

## 1D1 Organizations, cooperation for law enforcement

Category 1D1 Organizations, cooperation for law enforcement

2002-01-14 ISP Internet service providers association group security cooperation collaboration information sharing critical infrastructure protection law enforcement investigation

NewsScan

#### ISPs FORM A NEW ASSOCIATION

Several Internet companies have banded together to form a new group that will focus on compliance and liability issues. The U.S. Internet Service Provider Association (US ISPA) will replace the Commercial Internet eXchange, which is folding. Founding members of the new group including AOL, Cable & Wireless, Earthlink, eBay, Teleglobe, Verizon Online and WorldCom. US ISPA vice president Tom Dailey says the group will examine such issues as online security, liability and compliance with the new antiterrorism law, the USA-Patriot Act, and the Council of Europe Convention on Cybercrime. In addition, the US ISPA will raise "a variety of other policy and legal issues of concern to ISPs, such as Internet privacy, content regulations and intellectual property." (Wall Street Journal 14 Jan 2002)

http://interactive.wsj.com/articles/SB1011053572133523720.htm (sub req'd)

Category 1D1 Organizations, cooperation for law enforcement

2002-04-22 mandatory reporting computer crime government law enforcement police proposal

statistics knowledge base incidence rates risk management

Security Wire Digest 4 31

#### \*PROSECUTOR SAYS HACK ATTACKS MUST BE REPORTED

Companies need to come forward and admit when they've been hacked, urged U.S. prosecutor David Green at Microsoft's Government Leaders' Conference last week. So long as companies fail to report attacks, the government will be limited in its ability to find culprits and bring them to justice, said Green, the principal deputy chief of the Department of Justice's computer crime division. "We have to make the reporting of these attacks the norm. We need corporate cooperation to report these sorts of vulnerabilities to law enforcement in order that they are able to deal with it," he told delegates, according to a published report. A key, he added, is creating a public-private partnership that promotes trust and honors confidentiality. Congress is currently considering legislation that would exempt security information shared with the government from the Freedom of Information Act.

Category 1D1 Organizations, cooperation for law enforcement

2002-06-17 surveillance investigation law enforcement government legal guidelines Web tax

intelligence

Edupage

#### UK WEB SITE GUIDES LEGAL SNOOPERS

The British government has set up a Web site to advise qualified UK government departments and organizations how to stay within legal bounds in carrying out covert surveillance of British citizens' use of their telephones, fax machines, Web browsers, and e-mail accounts. Passage of the Regulation of Investigatory Powers Act in 2000 made it easier for customs, tax, police, and intelligence services to get permission to spy on criminals and citizens. The RIP Act removed the requirement to obtain permission for surveillance from a judge and put approval and oversight into the hands of the Office of Surveillance Commissioners. BBC, 17 June 2002

http://news.bbc.co.uk/hi/english/sci/tech/newsid\_2049000/2049593.stm

Category 1D1 Organizations, cooperation for law enforcement

2002-11-25 law enforcement police databases information linking coordination

NewsScan

#### LAW & ORDER DATABASES NEED BETTER LINKING

Criminologist Peter Scharf says it took too long to share information during the hunt for the snipers in the Washington area: "If these two guys could go undetected for 23 days, what about somebody with a nuclear bomb in Manhattan? The technology systems don't connect. We have an archaic patchwork of information sharing -- on the fingerprint level, on the ballistics level, on the field interrogation level." Only 34 states are directly linked to the FBI's Integrated Fingerprint Identification System database; those states are the only ones that can submit prints electronically and receive a response from the FBI within two hours if any print matches one in the bureau's files. (USA Today 24 Nov 2002)

Category 1D1 Organizations, cooperation for law enforcement

2002-12-13 law enforcement police search investigation public cooperation advertising

announcements warrants

#### NewsScan

#### A BANNER DAY FOR FBI'S MOST-WANTED BAD GUYS

The FBI's "10 Most Wanted" list has been on that agency's own Web site since 1995, but now it will get new life on pop-up banner ads on Web sites owned and operated by the Terra Lycos network. The ads are being displayed as a public service by Terra Lycos. (Computer Weekly 13 Dec 2002)

## 1D2 Technology for law enforcement

Category 1D2 Technology for law enforcement

2002-01-09 biometric face recognition I&A identification authentication failure removal law

enforcement police

RISKS 21 87

Nick Brown wrote in RISKS, "... [A] highly-publicised facial recognition system has been quietly dropped by law enforcement officials in Tampa, Florida, following a large number of false positives (including males identified as females, and vice versa) and a total of zero matches against known criminals, leading to zero arrests. Aside from the already-discussed civil liberties RISKs of such systems, it seems we need to add the possibility that the taxpayers may not be getting value for money, with or without their knowledge (the withdrawal of this kind of thing tends to be done with rather less media coverage than its introduction). One wonders if this will have any effect on plans to introduce such systems into airports to 'detect' terrorists." http://www.aclu.org/issues/privacy/drawing\_blank.pdf

Category 1D2 Technology for law enforcement

2002-01-20 computer forensics accounting fraud investigation scandal financial data

Security Wire Digest 4 5

#### ENRON SCANDAL PUTS FOCUS ON FORENSICS

Computer forensics will likely play a significant role in Congress' investigation into the financial collapse of Enron, since the bankrupt energy giant's accounting firm--Arthur Andersen--admitted destroying several potentially incriminating documents-including many e-mails and computer files. Authorities believe that at least some of the destroyed documents could help explain how Andersen could have approved several off-the-books partnerships--which hid billions in Enron debt--and are at the heart of the debacle. Enron has since fired Arthur Andersen. "Computer forensics is going to be very important in this investigation," says John Patzakis, president and general counsel for Guidance Software, maker of the EnCase forensics application. "There is so much that you can learn about a system, such as how it's been used. Even if these files are completely deleted, there's still a lot of information that can be gleaned, including when the deletions occurred."

Category 1D2 Technology for law enforcement

2002-01-20 content filtering analysis lying dissimulation dishonesty untruth law enforcement investigation forensic

NewsScan

#### SOFTWARE UNCOVERS E-MAIL UNTRUTHS

SAS Institute has developed software that it says can sift through e-mails and other electronic text to discern falsehoods. "The patterns in people's language change when they are uncertain or lying," says Peter Dorrington, business solutions manager at SAS. "We can compare basic patterns in words and grammatical structures versus benchmarks to detect likely lies." For instance, over-use of the word "or" and too many adjectives can be giveaways, according to Aldert Vrij's book, "Detecting Lies and Deceit." SAS says its software can also be used to detect inaccuracies in resumes and job applications. (Financial Times 20 Jan 2002)

http://news.ft.com/news/industries/internet&e-commerce

Category 1D2 Technology for law enforcement

2002-01-20 wireless secure network encryption police

Security Wire Digest 4 5

At Boston's Logan Airport, MA state troopers are successfully using secure wireless gadgets for rapid background checks. The Blackberry devices, equipped with PocketBlue software, use AES for encryption.

Category 1D2 Technology for law enforcement

2002-02-20 paper snail mail conversion e-mail law enforcement surveillance investigation

privacy security confidentiality vulnerability

NewsScan

#### NEW SERVICE DELIVERS PAPER MAIL ELECTRONICALLY

PaperlessPOBox offers a service that delivers 100% of your mail electronically, whether it starts out that way or not. Customers who sign up have their snail mail forwarded to an outside P.O. Box address, where it is picked up by PaperlessPOBox, scanned, and transmitted to users' e-mail accounts on the same day. The user receives exact replicas of whatever mail was sent, including hand-written notes and photos. "Personal notes translate very well," says PaperlessPOBox President David Nale. "We use state-of-the-art scanners." The service is targeted toward business travelers who have difficulty keeping up with overflowing mail boxes and received a boost last fall during the anthrax scare when people were fearful of contamination via paper mail. (Reuters 20 Feb 2002)

http://story.news.yahoo.com/news?tmpl=story&cid=581&u=/nm/20020220/tc\_nm/column\_nettrends\_dc\_14

Category 1D2 Technology for law enforcement

2002-02-21 consumer profiling audit trail logging tracking music video surveillance law

enforcement police investigation family parental control supervision

NewsScan

#### MICROSOFT TRACKS USERS' SONGS, MOVIES

The newest version of Microsoft's MediaPlayer software, which comes free with the Windows XP operating system, is designed to create a log of the songs and movies that users play. When a CD or DVD movie is played, the MediaPlayer 8 software stores that information in a file on the user's PC, in addition to transmitting an identifier number unique to each user on the computer. That function creates the possibility that information on user habits could be tracked and sold for marketing purposes. Privacy experts say the log file could be used by investigators, lawyers, snooping family members, or companies interested in finding out an individual's personal entertainment habits. Microsoft said the program creates the log so that a user does not have to repeatedly download the same track, CD or movie information, and that the ID number was created simply to enable MediaPlayer users to have a personal account on the Web site dealing with software. The company says it has no plans to share that information with others. (AP/Miami Herald 21 Feb 2002) http://www.miami.com/mld/miamiherald/2712422.htm

Category 1D2 Technology for law enforcement

2002-03-28 terrorism homeland security confidentiality anonymity surveillance

NewsScan

#### HIDING ON THE INTERNET

Terrorist groups are known to be heavy users of the Internet, so why isn't it easier to trace their whereabouts? David Lang, a computer forensics expert, explains: "The Internet presents two main challenges. One is it's ubiquitous -- you can access it from just about anywhere in the world. The other thing is you can be easily hidden." Terrorists capitalize on the first of those features by using Internet cafes and anonymous public kiosks to send mail, and exploit the second feature by making good use of encryption. One interesting fact is that terrorists don't seem to need the services of sites like Anonymizer.com that specialize in helping people send messages without revealing their identities. Lance Cottrell of Anonymizer points out the tension that exists between privacy and security: "That's kind of the irony in this. For the honest good citizen, privacy is extremely endangered and tracking is ubiquitous. But I don't see a sign that we've ever been able to build a system that criminals with serious intent haven't been able to circumvent." (New York Times 28 Mar 2002) http://partners.nytimes.com/2002/03/28/technology/circuits/28TERR.html

Category 1D2 Technology for law enforcement

2002-05-05 suspect profiling law enforcement police surveillance cameras artificial intelligence

pattern matching signatures

RISKS 22 05

Merlyn Kline contributed this Orwellian note to RISKS:

According to the UK broadsheet \*The Independent\*, Dr Sergio Velastin, of Kingston University's Digital Imaging Research Centre, has developed software to analyse CCTV images for the purpose of predicting crime:

http://news.independent.co.uk/uk/crime/story.jsp?story=287307

Quote from the article:

Scientists at Kingston University in London have developed software able to anticipate if someone is about to mug an old lady or plant a bomb at an airport. It works by examining images coming in from close circuit television cameras (CCTV) and comparing them to behaviour patterns that have already programmed into its memory. The software, called Cromatica, can then mathematically work out what is likely to happen next. And if it is likely to be a crime it can send a warning signal to a security guard or police officer.

Category 1D2 Technology for law enforcement

2002-05-18 profiling database errors QA quality assurance secrecy homeland security

RISKS 22 07

Adam Shostack contributed this thoughtful note to RISKS:

>Risks of mis-identification, arrest, etc, from law enforcement databases are well documented. The new, secret terrorism databases are starting to repeat these mistakes, as documented in a New Yorker article on a 70 year old black woman (Johnnie Thomas) is in a set of FBI databases, because "John Thomas Christopher" was an alias used by Christian Michael Longo, once on the FBI top ten most wanted list. Unfortunately for Johnnie Thomas, even the fact that Mr. Longo is in jail in Oregon hasn't removed her name from the computers, and the New Yorker article documents her (so far unsuccessful) attempts to clear her name.

http://www.newyorker.com/talk/content/?020513ta\_talk\_mcnamer

The application of fair information practices; allowing people to know what data is stored about them, to access and correct records, etc, is often brushed aside for law enforcement claims that the data must remain secret. Does anyone know if these databases are the the Expanded Computer Assisted Passenger Screening Program, or something else?

Category 1D2 Technology for law enforcement

2002-06-06 ISP Internet service provider wiretaps surveillance subpoena court order compliance

Security Wire Digest; Findlaw Download This

VERISIGN TO LAUNCH WIRETAPPING TOOL

VeriSign Inc. on Monday [in June 2002] announced a service to help telecommunications companies comply with federal wiretap regulations and orders. The company's NetDiscovery Service, scheduled to launch by the end of June, will help carriers comply with a 1994 law requiring them to have equipment that supports content-intercept orders. The 1994.

Communications Assistance for Law Enforcement Act requires that carriers have systems in place that allow law enforcement - with a court order - to quickly intercept phone calls and data.

http://news.findlaw.com/ap/ht/1700/6-3-2002/20020603153014\_08.html

Communications Assistance for Law Enforcement Act of 1994

http://caselaw.lp.findlaw.com/casecode/uscodes/18/parts/i/chapters/119/toc.html

4

44

Category 1D2 Technology for law enforcement

2002-06-06 Carnivor ISP Internet service provider e-mail traffic surveillance investigation

technology wiretaps flaws court order bungled

RISKS 22 11

The Electronic Privacy Information Center (EPIC) received information under a court order that revealed that the FBI's "Carnivore" software was misconfigured during an attempt to monitor traffic relating to Osama bin Laden. The resulting tide of unwanted information, including e-mail for unauthorized targets, so upset the FBI operative that he destroyed the entire run of data. A commentary by EPIC noted, "Since its existence became public in 2000, the Carnivore system has been criticized by EPIC and other privacy groups, as well as members of Congress, because it gives the FBI unprecedented, direct access to the data networks of Internet service providers. The FBI has publicly downplayed the system's potential for over-collection of private communications, although internal documents released earlier to EPIC confirmed such a risk. An independent review of Carnivore commissioned by the Justice Department also found that the system is capable of 'broad sweeps' and recommended technical changes to address the problem. Neither DOJ nor the FBI has indicated publicly whether those recommendations were ever implemented."

Category 1D2 Technology for law enforcement

2002-06-10 surveillance privacy terrorism homeland security audit trail

RISKS 22 12

\*The New York Times\* (2 Apr 2002) reported that investigators trying to determine how a New York woman had contracted Anthrax during last year's bioterrorist attack had used subway computer records and her fare card to trace her movements in the city prior to her death.

Category 1D2 Technology for law enforcement

2002-08-16 e-mail law enforcement police surveillance investigation archives fraud

NewsScan

#### PEOPLE SAY THE DARNDEST THINGS IN E-MAIL

In recent investigations e-mail is playing an increasingly pivotal role in producing criminal evidence. In the kidnapping and murder case of Wall Street Journal reporter Daniel Pearl, investigators used e-mail from his abductors to track them down, and anti-American sentiments voiced in messages from Taliban convert John Walker Lindh and shoe bomb suspect Richard Reid to their mothers were gathered as evidence against them. Closer to home, Merrill Lynch analysts indiscreetly derided stocks as a "disaster" or a "dog" in e-mail while publicly touting them to investors. "It's like the gift that keeps on giving," says a California deputy attorney general. "People are so chatty in e-mail." And e-mail seems to linger forever -- or at least until the space occupied by deleted files is overwritten with new information. "The best way to get rid of computer data is to take the hard drive and pound it with a hammer and throw it in a furnace," says the head of a forensic software company. And even that might not work -- those messages may still be stored on a corporate or ISP server, or on the recipient's computer. "E-mail has become the place where everybody loves to look," says Irwin Schwartz, president of the National Association of Criminal Defense Lawyers. (AP 15 Aug 2002)

http://apnews.excite.com/article/20020815/D7LDUU4O0.htm

Category 1D2 Technology for law enforcement

2002-10-01 surveillance eavedropping analysis government

NewsScan

#### NSA UPGRADES SOFTWARE FOR MONITORING INTERNET CHATTER

The National Security Agency has signed a \$282-million contract with Science Applications International Corp. in San Diego for new software designed to improve the Agency's abilities to sort through millions of electronic communications sent worldwide. Richard A. Best of the Congressional Research Service explains, "There's a ton more communications out there, and how to sift through that is an increasing problem for the NSA," for which it offers "profound 'needle-in-a-haystack' challenges." (AP/San Jose Mercury News 30 Sep 2002)

Category 1D2 Technology for law enforcement

2002-11-05 police law enforcement investigation text messaging alerts

NewsScan

#### GERMAN POLICE USE TEXT MESSAGING TO CATCH CRIMINALS

Police in Germany are taking part in a pilot project that makes use of SMS (short messaging service) technology to enlist the help of bus and taxi drivers in apprehending criminal suspects. Police send out text messages with descriptions of the person they are seeking and, if possible, a license plate number. The concept is being tested in ten cities over the next five months, and if successful, will be expanded nationwide. "It increases the likelihood of solving a crime immediately after it has been committed," says Ulrich Kersten, president of the Federal Bureau of Criminal Investigation. (Ananova 4 Nov 2002)

# 1D3 Litigation, legal rulings, judgements affecting law enforcement

Category 1D3 Litigation, legal rulings, judgements affecting law enforcement

2002-02-20 law enforcement e-mail interception forensics inspection authority warrant court

order lawsuit jurisprudence wiretapping

#### NewsScan

#### DO THE POLICE NEED A COURT ORDER TO INSPECT A SUSPECT'S E-MAIL?

In a case involving the admissibility of Internet evidence used to convict he a man for solicitation of a 15-year-old girl he met in a chat room, the Pennsylvania Supreme Court will decide whether police authorities need a court order (as they would if they wanted to set up a telephone wiretap operation) before looking at a suspect's e-mail and instant messages. The lower court took the position that the wiretapping law did not apply because the police did not intercept the messages but looked at them after they had been received, and it suggested that the defendant had given implied consent to the inspection of his messages: "Any reasonably intelligent person, savvy enough to be using the Internet, would be aware that messages are received in a recorded format, by their very nature, and can be downloaded or printed." (AP/USA Today 20 Feb 2002) http://www.usatoday.com/life/cyber/tech/2002/02/20/internet-wiretap.htm

Category 1D3 Litigation, legal rulings, judgements affecting law enforcement

2002-05-14 ISP Internet service providers subpoenas search warrants police officers physical

presence

#### NewsScan

#### INTERNET GROUPS SAY THEY DON'T WANT POLICEMEN IN THEIR LOBBIES

Internet service providers and trade groups have gone to a federal appeals court to protest another court's requirement that police officers be physically present when search warrants are conducted to find electronic messages or files. The groups argue that the requirement creates a "chilling effect" on a company's subscribers without accomplishing anything good: "The police officer waiting in the lobby while the technician works away on the computer does not in any way safeguard anyone's Fourth Amendment rights." Besides, it would be burdensome and disruptive: "A large Internet service provider can receive literally hundreds of search warrants and other requests for information during the course of a year. It is entirely possible that at any given time a dozen or more law enforcement officers would be on the premises of given service provider." (Reuters/San Jose Mercury News 13 May 2002)

http://www.siliconvalley.com/mld/siliconvalley/3256778.htm

Category 1D3 Litigation, legal rulings, judgements affecting law enforcement

2002-05-28 privacy surveillance subpoena just cause ISP telecommunications police law enforcement civil liberties homeland defense

FindLaw Download This 87

#### GOVERNMENT, INTERNET BIZ FIGHT TERROR

In the seven months since the passage of a sweeping law to combat terrorism, Internet and telecommunications companies have seen a surge in law enforcement requests to snoop on subscribers. Privacy advocates fear that expanded police power under the Patriot Act - combined with lax oversight and increased cooperation between the government and private sector phone network and Internet gatekeepers - may be stomping on civil liberties. The new laws do not apply just to terrorism but to other crimes as well.

http://news.findlaw.com/ap/ht/1700/5-27-2002/20020527044501\_18.html

Special Coverage -- War On Terrorism

http://news.findlaw.com/legalnews/us/terrorism/index.html

Category 1D3 Litigation, legal rulings, judgements affecting law enforcement

2002-07-09 jurisdiction wiretaps law legal application surveillance law enforcement police

investigation ISP Internet serfice provider phone cable

NewsScan

#### IS BROADBAND A TELECOM SERVICE -- OR AN INFO SERVICE?

The answer to that question will make a lot of difference, especially to the FBI and the Justice Department, which rely on a law requiring "telecommunications" services to be designed in a way that would allow law enforcement officials, with a court order, to monitor activity of suspected criminals or terrorists; in contrast, there is no such requirement for "information services." So the Federal Communications Commission will be asked to determine that electronic-surveillance access rules also apply to the broadband information offerings of phone and cable companies. (USA Today 8 Jul 2002) http://www.usatoday.com/life/cyber/tech/2002/07/09/wire

Category 1D3 Litigation, legal rulings, judgements affecting law enforcement

2002-07-16 surveillance wiretaps police law enforcement warrants court order criminal hackers

crackers life sentence punishment

NewsScan

#### HOUSE APPROVES LIFE SENTENCES FOR CRACKERS

The U.S. House of Representatives has approved the Cyber Security Enhancement Act (CSEA) by a near-unanimous vote. Among the Act's provisions are an expansion of police ability to conduct Internet or telephone eavesdropping without first obtaining a court order, and the approval of life prison sentences for malicious computer hackers (crackers) whose acts "recklessly" put others' lives at risk. In the case of wiretaps, the Act would permit limited surveillance without a court order when there is an "ongoing attack" on an Internet-connected computer or "an immediate threat to a national security interest." The surveillance would be limited to collecting a suspect's telephone number, IP address, URLs or e-mail header information -not the content of an e-mail message or phone conversation. In addition, the Act would permit ISPs to disclose the contents of e-mail messages and other electronic records to police in cases when "an emergency involving danger or death or serious physical injury to any person requires disclosure of the information without delay." The Act is not expected to meet any serious opposition in the Senate. (CNet News.com 15 Jul 2002)

http://news.com.com/2100-1001-944057.html?tag=fd\_top

Category 1D3 Litigation, legal rulings, judgements affecting law enforcement

2002-10-07 international criminal hacker consultants fraud conspiracy sting entrapment

monitoring surveillance sniffing keystroke logging court trial prosecution sentence

prison

NewsScan

#### RUSSIAN CAUGHT BY FBI STING GOES TO JAIL FOR COMPUTER CRIMES

Twenty-seven-year-old Russian computer hacker Vasily Gorshkov came to the U.S. for a job interview, but the interview was part of a sting operation to apprehend Gorshkov and another programmer for computer crimes, fraud and conspiracy. The two Russians complied with a request by the bogus interviewers to demonstrate their hacking skills, and when they used their passwords to hack into a computer network in Russia the FBI secretly logged those passwords to gather evidence against the pair. Gorshkov has just been sentenced to three years in a U.S. federal prison. (VNUnet 7 Oct 2002) http://www.vnunet.com/News/1135691

## 1D4 Government funding for law enforcement

Category 1D4 Government funding for law enforcement

2002-05-21 cybercrime research funding law legislation

FindLaw Download This 86

#### SENATE PANEL OKS MORE CYBERCRIME DOLLARS

The U.S. Senate Commerce Committee today voted to increase funding for anti-cybercrime programs, despite claims from software and high-tech groups that last-minute changes to the bill could stifle innovation. The "Cyber Security Research and Development Act," sponsored by Sen. Ron Wyden, D-Ore., would give \$970 million over five years to the National Science Foundation and National Institute of Standards and Technology to improve government computer and network security. http://www.newsbytes.com/news/02/176661.html

Category 1D4 Government funding for law enforcement

2002-10-09 federal funding grant institute cyberterrorism research

NewsScan

#### CARNEGIE MELLON GETS GRANT TO FIGHT CYBERTERRORISM

Carnegie Mellon's new Center for Computer and Communications Security has received \$35.5 million in funding from the U.S. Defense Department to further its goal of developing tools and tactics for fighting cyberterrorism. The Center is already researching ways to integrate artificial intelligence into computer hardware so that components such as hard drives could automatically shut down in event of hacker attack and even report such attacks to network administrators. Researchers are also investigating how to use biometric technology, such as fingerprints, iris and voice scans, and face recognition, to confirm the identity of computer system users. (AP 8 Oct 2002)

http://apnews.excite.com/article/20021008/D7MHJA6G0.htm

## 21.1 General QA failures

Category 21.1 General QA failures

2002-01-04 QA quality assurance automated teller machines ATM bank data corruption error

ug

RISKS 21 84, 87

Paul van Keep reported to RISKS on a drastic programming error in the Netherlands just as the currency switched to the Euro:

"About 51,000 customers who withdrew money from their ING Bank account on 1 & 2 Jan 2002 (through an ATM) have had the wrong amount debited from their account. The bank hasn't yet given an explanation for the error other than to suspect that it was related to the high stress their systems were under during the first few days of the new year. The amounts debited from customer accounts was a hundred times what they withdrew from the ATMs. This got some people into trouble when their balance went negative and they could no longer use their bank PIN card to pay with in shops. ING Bank corrected the error yesterday."

Category 21.1 General QA failures

2002-01-06 QA quality assurance Euro conversion

RISKS 21 86

Clive Page told RISKS readers of a serious quality assurance problem in England: "Although the UK is one of the three European Union countries not to have adopted the Euro, many large retailers in the UK announced that they would accept them, but would give change in pounds sterling. Among these was the Debenhams chain of department stores. . . . Robert Sheilds, a 15-year old Luton schoolboy, decided he would like experience of using Euro, so he changed 10 pounds to Euro at a bank, and went on to his local branch of Debenhams to spend them. He found that they had programmed their tills as if there were 1.6 pounds to the Euro rather than 1.6 Euro to the pound, but none of the sales assistants was experienced enough to notice the error. So after his initial purchase, he still had more than 10 pounds in change. He tried to tell the store staff of their mistake, but they said the rate was programmed into the computer, and nobody had the authority to change it. So he carried on spending, and after two hours, ended up with 130 pounds of goods, and 20 pounds in cash. At this point the store manager asked him to leave, saying «I think you've had your fun». Richard then took a train to Bedford (about 20 miles away) to try his luck at another branch, but by this time staff had been alerted, and refused all Euro transactions."

Category 21.1 General QA failures

2002-01-10 b

bank interest calculations changes information warfare QA quality assurance design customer relations technical support failure incompetence stupidity obfuscation dolts publicity audit

RISKS; http://www.mit.edu/people/jik/pfsb\_problem/

86

Jonathan Kamens noticed a discrepancy in the interest calculations on his bank account one month as a result of a software upgrade (he was slightly overpaid). It took five months for the bank to explain the difference. In the meantime, Kamens put up a Web site that provided a great deal of embarrassing publicity and even humiliation for the bank officials who had been unable to deal with his simple request. [Moral: in the age of the Web, horrible customer service can cost you much more than the loss of one client's business.]

Category 21.1 General QA failures

2002-01-10 QA quality assurance design support flaws features failures incompetence stupidity foolishness crash data corruption

RISKS 21 86

Rex Black wrote in to RISKS with an off-the-top-of-his-head list of obvious quality assurance and design failures and bloopers from his recent experience. Some key points summarized (not literal quotes) from his list:

- \* Too many programs are written with no consideration of the possibility of data corruption in their data files. They ought to have recovery capabilities.
- \* Products are designed so that there are sometimes no error or diagnostic messages at all when they fail.
- \* Automatic updates of software can sometimes wipe out laboriously constructed configurations, making the updated version useless.
- \* Long-established problems that are known to technical support fail to make into even the electronic read-me files for their products.
- \* "The daily (or more often) crash that my Windows Me laptop computer subjects me to, generally without warning, usually losing a good fifteen minutes worth of work. I guess I should learn to save every thirty seconds?"

Mr Black ends with, "If experienced people like me have problems like this, imagine the average computer user who has no idea whatsoever about what is going on when her system screws up. And why should they have to understand a computer to use them? (Don Norman, in his book \*The Invisible Computer\*, discusses this situation at length.) Ultimately, a computer is a tool, nothing more, nothing less. I think we have a long way to go before we can claim levels of quality consistent with what the makers of almost any other tool could claim."

Category 21.1 General QA failures

2002-01-16 QA quality assurance data input bounds checking limits edits output verification

RISKS 21 87

Carl Fink contributed this gem to RISKS: "A Georgetown, TX man who had arranged for his water bill to be automatically debited from his bank account alertly noticed that his monthly bill was for over \$21,000. (If he hadn't noticed, the debit would have happened, causing him to bounce multiple checks before the error was corrected.) When he told the city of the problem, «They said there was absolutely nothing they could do to stop the automated debit, and it was out of their hands.» Their solution was to send a city employee with a check for \$21,000 to reimburse their customer! http://www.austin360.com/statesman/editions/tuesday/metro\_state\_1.html

Risks? Lack of sanity checking on a new billing system springs to mind. Lack of any way to correct errors is also quite prominent.

Category 21.1 General QA failures

2002-01-19 **QA** quality assurance design human error

RISKS 21 87

Arthur Goldstein reported, "The Chesterfield and North Derbyshire Royal Hospital admitted on 10 Jan that it had mistakenly sent computer generated letters to 30 patients, including six elderly men, telling them they were pregnant. The system operator was blamed for choosing the wrong option (instead of informing them that their operations had been postponed)."

[MK comments: Of course it isn't the operator's fault that there was a glitch; program designers are supposed to take input errors into account and to compensate for them. The designers should have included gender-specificity, age constraints, and so on in their design; e.g., {IF gender = male AND condition = female-specific THEN error}.

MORAL: Use table-driven checks to validate human inputs.]

Category 21.1 General QA failures

2002-02-01 quality assurance security reliability development Microsoft oxymoron

NewsScan

#### GATES REFLECTS ON FUTURE HOPES AND PAST SINS [12 Nov 2001]

Microsoft Chairman Bill Gates says his two top priorities now are improving the reliability of his company's software and conquering the market for "tablet" computers, the laptop-size computers that can be used like a clipboard. The tablets can be written on with a special stylus, and the writing is then treated by Microsoft software as though the words had been typed. Gates says tablet PCs will overtake laptops by 2005. As for software reliability, Gates is repentant: "We're doing a little bit of mea culpa on this. These are areas where Microsoft needs to improve. It affects the way we develop code." (USA Today 12 Nov 2001)

http://www.usatoday.com/life/cyber/tech/review/2001-11-12-comdex-gates.htm

#### MICROSOFT MAKES SECURITY A TOP PRIORITY [16 Jan 2002]

Microsoft Chairman Bill Gates says it's time to shift away from focusing on features to ensuring more security and privacy. Calling the new initiative "Trustworthy Computing," Gates wrote in an e-mail to employees, "When we face a choice between adding features and resolving security issues, we need to choose security. Our products should emphasize security right out of the box." Gates also emphasized that privacy should be a concern: "Users should be in control of how their data is used. It should be easy for users to specify appropriate use of their information, including controlling the use of e-mail they send." The new focus comes on the heels of a widely publicized security flaw in its flagship Windows XP program. (CNet News.com 16 Jan 2002)

http://news.cnet.com/news/0-1003-200-8509737.html?tag=mn\_hd

#### MICROSOFT HIRES SECURITY SPECIALIST [1 Feb 2002]

Microsoft has hired a top security expert who will oversee the development of company strategies to enhance the security of Microsoft's products, services and infrastructure. Scott Charney, a principal for PricewaterhouseCoopers' Cybercrime Prevention and Response Practice, called his new job "in a word, irresistible." Microsoft CTO Craig Mundie said Charney would be a valuable addition to the company: "As one of the industry's top computer security experts, Scott has wide-ranging experience in cybercrime and computer forensics, which will make him an essential member of Microsoft's Trustworthy Computing leadership team." (AP 1 Feb 2002)

http://apnews.excite.com/article/20020201/D7HD1SFO0.html

Category 21.1 General QA failures

2002-03-11 real time control system version upgrade failsafe QA quality assurance management

RISKS 21 94

RISKS moderator Peter G. Neumann summarized a case of inappropriate use of control software coupled with lack of management concern over safety issues in a railway accident in Michigan:

Operating with a less-than-a-year-old remote-controlled system, a runaway train plowed through NIPSCO's Michigan City Generating Station on the morning of 7 Mar 2002, hitting another locomotive before the second locomotive's engineer narrowly jumped to safety. The unmanned eastbound diesel-electric engine, known as Big Blue, was pushing six coal cars when it approached the coal drop-off area at about 30 m.p.h. at 7:15 a.m. However, the train (in excess of 1.5 million pounds, including the coal) did not respond to radio controls and smashed through the enclosed thaw shed and coal rotary dumper, before smashing into the other train, Old No. 12. (Big Blue should have been going only about 1 mph for the last 100 yards entering the dumper.) The impact sent the other train through a fence, uprooted a bumper post, and ripped up track. A spokesman blamed it on a switch malfunction. But the system was supposedly designed so that if the remote-controlled engine receives no signal, its brakes should automatically engage. Employees reportedly said that the system was not designed for the engines currently in use. Two other accidents occurred in the past month. Also noted was what sounds like a serious lack of receptivity from NIPSCO in responding to safety complaints from the workers' union over the past four or five years.

Category 21.1 General QA failures

2002-04-22 Y2K QA quality assurance repayments accounting errors

RISKS 22 04

In Brevard County, FL, several city administrations were reeling in shock when they were informed that due to problems during the run-up to the year 2000, they had been significantly overpaid by the County. Some small towns were facing repayments of up to 10% of their annual budget.

Category 21.1 General QA failures

2002-05-05 QA quality assurance billing utility electricity meter computer court disaster

response public relations failure

RISKS 22 05

Some customers of Seattle City Light have been billed up to 10 times the correct amount for their electricity. Although the municipal administration claimed it would adopt the "Nordstrom way" by dealing with billing disputes quickly and in favor of the customers, a spokesperson also said that electric meters don't lie, and thus at least one customer who had protested his bill had to prove that he did not use the power. [MK notes: hellooo? Computers often lie when they are programmed wrong. Claiming that a computer-generated result must be true because the computer says it is reminds one of the touching faith some children have in the Tooth Fairy.]

Category 21.1 General QA failures

2002-05-05 automated inventory control model overshoot exception QA quality assurance

statistical quality control

RISKS 22 05

Paul Breed told a cute story in RISKS:

>I've been working on an old car, in the process of removing the spot welds I needed a specific sized bullet tipped drill bit. The bit would only last about 5 welds and I had hundreds to do. The only place I could find locally to buy the bits was in a pack of 15 various size bits at the local home center.

So, over the period of three months, I purchased all of their drill sets, every weekend (usually 3 sets). Now I have disassembled the old car and don't need more bits. The last time I was in the home center they had so many of these drill bit sets that they were overflowing on to the floor.

From my experience the computerized inventory system has a delay of about 3 months. It determined that this item sold out for 12 weeks straight, plugged this into it's inventory tracking prediction S/W and ordered hundreds and hundreds of sets......

[MK comments: The spike in demand was so unusual it should have triggered a request for a human being to check on whether the automated system really should order so many replacements. Designers of automated systems should program statistical quality-control features into their software.]

Category 21.1 General QA failures

2002-05-22 Web design QA quality assurance public relations breach contract fraud

misrepresentation bait-and-switch class action lawsuit

RISKS 22 08

Tudor Bosman reported in RISKS: >Despite its initial denials, Compaq Australia now admits that it did in fact process the payments of customers who bought Presario laptops for just one cent as a result of an online pricing hiccup. [...] Compaq is still adamant, however, that it is not obligated to honor the accidental one-cent pricing, despite mounting industry criticism and ongoing threats of a customer-initiated class action law suit. [...] "As this was a genuine error, Compaq canceled all orders from the system. In instances where 1 cent was debited from customers accounts it will be refunded." <

Category 21.1 General QA failures

2002-05-22 program design QA quality assurance automated dispenser bounds checking

violation array initialization price error

RISKS 22 08ff

Several RISKS correspondents had a feast recounting stories of badly programmed vending machines. In one case, a user could lose money by punching in a choice too quickly after giving the no-armed bandit his dollar; slower-witted customers did fine [MK notes: this is an example of a "race condition" in programming, in which the programmer assumes that certain independ actions will necessarily occur in a strict sequence. The appropriate design is to serialize the components of the transaction; e.g., by using manually-coded semaphores or existing lock routines.] Another case involved unprogrammed values in the selection codes for chocolates; even though the machine typically had only 10 types of candies numbered from 1 to 10, nothing prevented entry of higher values (e.g, 80), and some of these numbers dispensed candybars with very low prices. [MK notes: any bets on the reasons for these bugs? Sure look like omission of bounds-checking (shouldn't accept position numbers higher than what's been filled) coupled with failure to initialize elements of an array (perhaps random values left over from quality assurance testing – if you can call it that in these circumstances).]

Category 21.1 General QA failures
2002-05-23 user interface design failure confusion ergonomics
RISKS 22 09

Chris Brady continued his analysis of the trouble at Swanwick airport in Britain:

Confusing screens at Swanwick's new air-traffic control centre near Heathrow have resulted in aircraft being directed towards the wrong airports. Controllers have also misread the altitude of aircraft because letters and numbers are difficult to distinguish on the screens, according to the \*Daily Mail\*, 23 May 2002. For example, the numbers 0, 8 and 6 are confused, leading to mistakes of thousands of feet in the height of flightpaths (noted in a report in \*Computer Weekly\* magazine).

Controllers and their supervisors at the privatised NATS (National Air Traffic Services) centre at Swanwick have detailed the errors in a health and safety report, which revealed that one controller has repeatedly misread requested flight levels, and mixed up FL360 (36,000 ft) with FL300 (30,000ft).

Others reported difficulties of seeing some letters clearly, particularly the Glasgow code EGPF and the Cardiff code EGFF.

NATS and the CAA (Civil Aviation Authority, U.K.) have said that difficulties in reading screens has been experienced only by a small number of controllers, and that it is not a safety matter. NATS also said that an improved display had been developed and a prototype was shortly to undergo testing.

The risks are many and unfortunately obvious. But what happened to the principles of good HCI design (human-computer interface) and user acceptance testing? Obviously no-one thought to ask the controllers if they could actually read the screens clearly as they play three-dimensional chess with the aircraft and passengers flying into, out of, and past one of the busiest airports in the world.

Category 21.1 General QA failures
2002-05-23 air-traffic control system failure crash availability upgrade maintenance disruption real-time

RISKS 22 09

Chris Brady reported in RISKS:

Yet again the new multi-million-pound air-traffic computer system at Swanwick near Heathrow crashed last Friday (May 17, 2002) shortly after 6.30 am.

This is a time of maximum inbound flights from the Middle and Far East -- with full 747's arriving at one a minute. Also too it is just when the morning rush hour for domestic and European departures and arrivals begins to build up.

The crash was the result of a 'routine upgrade' which made half the air traffic controllers' computer screens inoperable. This meant that only half the normal flights could be handled. This meant that airlines had to cancel most of their flights into and out of Heathrow - a situation which lasted for most of the day. Imagine one flight being canceled and all the disruption that can cause, then multiply that by many hundreds. And the knock on effect of the wrong planes and crews in the wrong places at the wrong times lasted for most of the following weekend. The consequent loss of revenue to the struggling airline industry is inestimable, to say nothing of the increased loss of confidence in the safety of flying amongst the traveling public.

The risks are obvious. The new computer system at Swanwick is a disaster waiting to happen. A 'routine upgrade' should not result in a major loss of service. The upgrade was obviously made to the primary system before testing on any back up system (is there one?), and if a routine upgrade can cause such a system loss then what would happen to a major upgrade?

Confidence in the safety of the ATC system at Heathrow is not increased with the U.K. Government's refusal to financially bale out - yet again - to the tune of millions of pounds - the owners of the new system, the privatised NATS (National Air Traffic Services).

Category 21.1 General QA failures

2002-06-27 documentation assumption error training awareness error

RISKS 22 13

Steve Bellovin summarized an unfortunate case of dependence on the wrong assumption when operating a computercontrolled military device:

According to a U.S. Army report, a software problem contributed to the deaths of two soldiers in a training accident at Fort Drum. They were firing artillery shells, and were relying on the output of the Advanced Field Artillery Tactical Data System. But if you forget to enter the target's altitude, the system assumes a default of 0. (A Web site I found indicates that (part of) Ft. Drum is at 679 feet above sea level.) The report goes on to warn that soldiers should not depend exclusively on this one system, and should use other computers or manual calculations.

Other factors in the incident include the state of training of some of the personnel doing the firing. [Source: AP]

## 21.2 Security product QA failures

Category 21.2 Security product QA failures

2002-01-04 QA quality assurance bug date javascript display

RISKS 21 85

William Colburn, writing in RISKS, noted an embarrassing date problem on the Web page showing McAfee virus alerts: the date was missing in the sentence, "This page current as of." With javascript enabled, the date shown was January 4, 1971. Worse still, it turned out that the 1971 date was pulled from his own computer, which had the wrong date set. Finally, he pointed out that the current date was inserted by javascript into a cached copy of the page, producing the risk that an old page with inaccurate information could mislead someone into thinking it was up to date.

Category 21.2 Security product QA failures

2002-01-20 antivirus anti-malware flaw quality assurance QA denial-of-service DoS crash Windows patch

Security Wire Digest 4 5

#### F-SECURE REPAIRS GLITCH

F-Secure last week fixed a problem in its Anti-Virus 5.30 that caused some Windows systems to crash. The flaw affects systems using Windows 9x/ME/NT/2000 and is caused by the way F-Secure Anti-Virus 5.30 deals with "certain combinations of strange or unusual characters." Though the problem affects very few customers, according to published reports, users who experience "occasional system crashes with complex and long hyperlinks, random blue screens on Microsoft Windows NT 4.0/2000 and false virus alarms" are encouraged to read the F-Secure advisory.

http://www.f-secure.com/support/top-issues/avwrks-top-issues-page\_2002011000.shtml

Category 21.2 Security product QA failures

2002-03-10 buffer overflows vulnerabilities ICAT CVE

#### **ICAT** Metabase

The ICAT Metabase < http://icat.nist.gov/icat.cfm > for the Common Vulnerabilities and Exposures (CVE) database reported 240 vulnerabilities involving buffer overflows out of a total of 1241 for the period from 1 Jan 2001 to 10 Mar 2002. This represents about 19% of all vulnerabilities logged for that period. Overall, for the entire period since the CVE began recording vulnerabilities in 1995, buffer overflows are named in 737 of the 3677 vulnerabilities or about 20% of the total.

Category 21.2 Security product QA failures

2002-04-22 privacy confidentiality design disclosure flaw QA quality assurance identity theft

SSN

RISKS 22 04

Ted Lee reported this astounding blunder in RISKS:

>I had reason to question the denial of a claim on our dental insurance. I called the appropriate 800 number and ended up choosing the menu item for their "automated services." The first thing they asked for was my subscriber identification number, which the voice then said "is usually your social security number." I punched it in. The voice repeated it back to me -- and then went on to spell out my name (yes, they had it correct; OK, no middle initials, but first and last name were fine) \*and\* give my birthdate. Need I say more?<

[MK adds: For those puzzled by the implications, this system allows anyone who has picked up a potential identity-theft victim's SSN and knows they do business with this insurance company to determine the victim's birthdate -- very helpful in developing the stolen identity.

MORAL: don't program automated systems to divulge confidential information unnecessarily.]

### 22.1 DoS attacks

Category 22.1 DoS attacks

2002-01-24 information warfare DoS denial-of-service attack disaster ISP Internet service

provider bankruptcy

Security Wire Digest 4 6

#### NO SILVER LINING FOR CLOUD NINE

Citing "a brazen act of cyberterrorism" U.K.-based ISP Cloud Nine ceased operations this week after being hit by a crippling denial-of-service attack. The network needs to be rebuilt as a result of the attack and the company's insurance won't cover the repairs. So, the ISP will either be sold or placed in the hands of administrators, CEO Emeric Miszti said in published reports. Cloud Nine's clients will likely be acquired by ISP V21.

http://www.ispreview.co.uk/cgi-bin/ispnews/viewnews.cgi?newsid1011696274,91619,

http://www.ispreview.co.uk/ispnews/comments/1011716173,95410,.shtml

Category 22.1 DoS attacks

2002-04-04 DoS denial-of-service attack malformed packet PKC public key cryptosystem IPSec

bug flaw design QA quality assurance

Security Wire Digest 4 26

The OpenBSD ISAKMPD IPSec keying daemon was found to have a design flaw that allowed a denial-of-service attack through malformed packets. A patch was quickly issues. However, Kurt Seifried of Security Wire Digest pointed out that the test suites used for quality assurance in public key cryptography tend not to include the possibilities of DoS attacks.

Category 22.1 DoS attacks

2002-04-25 malformed packets DoS denial-of-service attack BSOD blue screen of death kernel

panic Windows 2000 endless loop default settings TCP/IP

Security Wire Digest 4 32

\*PORT 445 ATTACK COULD CAUSE DoS

By Shawna McAlearney

Security researchers are warning users to change default registry settings on Windows 2000 boxes to prevent denial-of-service (DoS) attacks through TCP port 445.

Researcher Peter Grundl of KPMG Denmark says that sending malformed packets to the Microsoft-ds port (TCP 445) can result in kernel resources being allocated by the LAN Manager service, which manages domain access. The consequences of such an attack could vary, from the Windows 2000 host ignoring the attack to users finding the dreaded blue screen of death. Experts say the impact of the attack would likely depend upon which services were running.

Targeting the Windows 2000 Server/Advanced Server/Professional, Grundl says: "An attack could be something as simple as sending a continuous stream of 10K null characters to TCP port 445." According to the advisory, this attack will cause the system service to enter a state where it constantly uses 100 percent of CPU resources.

"Port 445 attacks are a recurring problem for users of Windows 2000," says Steve Gibson, president of Gibson Research Corp. "Luckily, any NAT or firewall will protect against the whole class of port 445 vulnerabilities."

Microsoft says it has confirmed this is a problem. The software giant recommends concerned users follow the Registry Editor instructions provided on its Web site, but warns that using the Editor incorrectly can cause serious problems that may not be fixable.

http://support.microsoft.com/default.aspx?scid=kb;en-us;Q320751

Category 22.1 DoS attacks

2002-05-05 **DoS** denial of service government information warfare

#### NIPC Daily Report

The White House Web site reportedly suffered a brief but crippling denial of service attack that rendered the site inaccessible to users on 4 May. White House spokesperson Jimmy Orr confirmed that the White House site was rendered inaccessible due to a "denial of service" in the morning hours between 9 a.m. and 11:15 a.m. EDT. [Spokespersons could not attribute the denial of ] service to an orchestrated attack, but did confirm that the White House was "looking into" the possible causes of the of the shutdown. Technicians were able to "unclog the clog" between Whitehouse.gov and its Internet service provider, making the site accessible to the general public. At no point did any malicious data reach White House servers. Security experts believe the Whitehouse.gov shutdown to be linked to the spate of Web site hacks and defacements launched by Chinese and pro-Chinese Internet vandals over the past few days. (Source: Newsbytes, 5 May)

Category 22.1 DoS attacks

2002-08-07 infowar information warfare international attack Internet denial-of-service DoS ISP

Internet service providers

#### NewsScan

#### FAILED ATTACKS ON INTERNET

Attacks on U.S. Internet providers Tuesday morning [Aug 6] turned out to be just a blip on the screen. Bush Administration cybersecurity chief Richard Clarke described the attacks -- which were thought to have come from someplace in Western Europe -- as amounting to not much more than an "unusual" event: "There was a real spike in Internet traffic at odd hours. It was clearly unusual because it was five times and seven times normal, but it didn't take anything down." Internet monitoring group Matrix NetSystems detected a 1% decrease in Internet accessibility within the hours of the attacks, but most U.S. systems managers say the attacks were barely noticeable and caused no damage. (AP/New York Times 6 Aug 2002) http://www.nytimes.com/2002/08/07/technology/07HACK.htm

Category 22.1 DoS attacks

2002-10-23 criminal hackers attack denial-of-service DoS DNS Domain Name System root

servers

#### NewsScan

#### HACKER ATTACK TARGETS ROOT SERVERS

A powerful denial-of-service attack briefly crippled nine of the 13 Internet "root" servers, but traffic routing was able to continue unimpeded, said ICANN VP Louis Touton: "As best we can tell, no user noticed and the attack was dealt with and life goes on." One government official described Monday's attack as the most sophisticated and large-scale assault on these root servers to date. The attack, which began around 4:45 p.m. EDT on Monday, blasted the servers with 30 to 40 times the normal amount of messages, rendering seven computers unable to respond to legitimate Internet traffic. Two others failed intermittently during the attack. The Internet theoretically can run with just one operational root server, but response times would be very slow. (AP 23 Oct 2002)

http://apnews.excite.com/article/20021023/D7MR8PT00.htm

Category 22.1 DoS attacks

2002-11-06 DNS Domain Name System root servers vulnerabilities attacks protection

#### NewsScan

#### VERISIGN TAKES STEPS TO PROTECT ROOT SERVERS

Verisign has taken steps to protect the two root servers that it controls, following last month's attack that briefly crippled nine of the 13 computer servers that manage global Internet traffic. The company says it moved one of its computers to a different building in an unspecified location in northern Virginia and onto a different part of its network. Verisign says the change is designed to ensure that a hardware outage or focused attack targeting part of its network could not disrupt both servers. FBI Director Robert Mueller said last week that the October 21 attacks have been traced back to hacked computers in South Korea and the U.S. (AP/Los Angeles Times 6 Nov 2002)

## 22.4 Accidental availability disruptions

Category 22.4 Accidental availability disruptions

2002-02-15 availability denial of service quality assurance service level agreement contractual obligation liability e-mail delivery reliability

NewsScan

#### COMCAST: 'NOT 100% READY' TO DEAL WITH CUSTOMER PROBLEMS [4] an 2002]

Internet service problems were experienced by about 10% of 71,000 Comcast Cable customers in North Jersey who had been transferred to Comcast's own network after the failure of one offered by Excite@Home. "These kinds of problems are very typical when you're launching something new... Our folks were dealing with a large amount of calls at a single point in time. There were some early folks we brought on that were not 100% ready for everything customers were asking," says a company spokesperson. (New York Times 4 Jan 2002)

http://partners.nytimes.com/2002/01/04/technology/04COMC.html

#### COMCAST PROBLEMS AFFECT DELIVERY OF 300,000 MESSAGES [15 Feb 2002]

Comcast, the cable company and Internet service provider, said yesterday it would "work around the clock" to fix a technical problem that slowed delivery of 300,000 subscriber messages. Industry observers remember that when Excite@Home was on the way to declaring bankruptcy last year it had tried forcefully to make the point that cable companies Comcast and AT&T did not understand the complexity and costs of operating an Internet business. (New York Times 15 Feb 2002) http://partners.nytimes.com/2002/02/15/technology/15PRIV.html

Category 22.4 Accidental availability disruptions

2002-02-20 documentation DNS Domain Name System reserved addresses DoS denial-ofservice

RISKS 21 92ff

Gene Spafford wrote about an interesting problem that occurred in late 2001 when e-mail to one of his friends starting timing out. Investigation revealed that some forbidden origination addresses taken from the IANA list of reserved IP ranges were now being used legitimately. Spafford warned fellow system administrators to keep track of such changes regularly to avoid similar inadvertent self-inflicted denial of service.

James Graves chimed in with a thoughtful comment on the importance of keeping an up-to-date central database of operations knowledge so that problems can be solved once and then later occurrences can be solved immediately simply by looking up the solutions.

Category 22.4 Accidental availability disruptions

2002-03-31 QA quality assurance DoS denial of service disaster availability

RISKS 22 02

Lindsay Marshall reported in RISKS, >Barclays BACS payment system failed last week, and a large number of people did not get their pay check in their bank account. Normally this would not be a huge problem, but because it is Easter and so has two bank holidays leading up to the last day of the month it is a huge disaster.<

Category 22.4 Accidental availability disruptions

2002-04-08 QA quality assurance operations merger combination bank financial systems failure payments errors debits transactions availability

RISKS 22 03FF

A series of reports in RISKS noted that the merger of the 12 largest banks in Japan had caused a number of problems, including, "more than 30,000 transaction errors and 2.5 million delayed debits" and "2.5 million of the 3 million automatic debits scheduled to be processed on 1 Apr 2002, including utility and credit card bills, couldn't be made on that day".

Category 22.4 Accidental availability disruptions

2002-04-22 credit card processing disaster recovery outage downtime customer service quality training intelligence stupidity obtuse pig-headed snot-nosed heap parrot droppings

RISKS 22 04

In April 2002, Citibank VISA experienced a system error that prevented customers from paying their bills on the Web. When Bill Brykczynski tried to pay his bill by phone from his checking account, he found that the phone-based systems were also down, preventing the customer service people from taking his payment. A few days later, still unable to pay his bill using the Web, he called customer service again. This time, the agent asked him for a check number even though there was no check involved. Although Mr Brykczynski tried to explain that giving a check number in this case made no sense, the agent was having none of it. Brykczynski gave up. [MK writes: (1) have a disaster plan in place; (2) train your customer service people to THINK before they refuse an explanation.]

## 23.1 Java

Category 23.1 Java

2002-03-10 Java vulnerabilities ICAT CVE

ICAT Metabase

The ICAT Metabase < http://icat.nist.gov/icat.cfm > for the Common Vulnerabilities and Exposures (CVE) database reported the following vulnerabilities involving Java for the period from 1 Jan 2001 to 10 Mar 2002:

CAN-2000-1117: The Extended Control List (ECL) feature of the Java Virtual Machine (JVM) in Lotus Notes Client R5 allows malicious web site operators to determine the existence of files on the client by measuring delays in the execution of the getSystemResource method. Published Before: 1/9/2001 Severity: Low

CAN-2001-0068: Mac OS Runtime for Java (MRJ) 2.2.3 allows remote attackers to use malicious applets to read files outside of the CODEBASE context via the ARCHIVE applet parameter. Published Before: 2/12/2001 Severity: Medium

CAN-2001-0186: Directory traversal vulnerability in Free Java Web Server 1.0 allows remote attackers to read arbitrary files via a .. (dot dot) attack. Published Before: 5/3/2001 Severity: High

CAN-2001-0297: Directory traversal vulnerability in Simple Server HTTPd 1.0 (originally Free Java Server) allows remote attackers to read arbitrary files via a .. (dot dot) in the URL. Published Before: 5/3/2001 Severity: Low

CAN-2001-0307 Summary: Bajie HTTP JServer 0.78 allows remote attackers to execute arbitrary commands via shell metacharacters in an HTTP request for a CGI program that does not exist. Published Before: 5/3/2001 Severity: Medium

CAN-2001-0308: UploadServlet in Bajie HTTP JServer 0.78 allows remote attackers to execute arbitrary commands by calling the servlet to upload a program, then using a ... (modified ..) to access the file that was created for the program. Published Before: 5/3/2001 Severity: Medium

CAN-2001-0324: Windows 98 and Windows 2000 Java clients allow remote attackers to cause a denial of service via a Java applet that opens a large number of UDP sockets, which prevents the host from establishing any additional UDP connections, and possibly causes a crash. Published Before: 5/3/2001 Severity: High

CAN-2001-0926: SSIFilter in Allaire JRun 3.1, 3.0 and 2.3.3 allows remote attackers to obtain source code for Java server pages (.jsp) and other files in the web root via an HTTP request for a non-existent SSI page, in which the request's body has an #include statement. Published Before: 11/28/2001 Severity: Medium

CAN-2001-1008: Java Plugin 1.4 for JRE 1.3 executes signed applets even if the certificate is expired, which could allow remote attackers to conduct unauthorized activities via an applet that has been signed by an expired certificate. Published Before: 8/31/2001 Severity: High

CVE-2000-1099: Java Runtime Environment in Java Development Kit (JDK) 1.2.2\_05 and earlier can allow an untrusted Java class to call into a disallowed class, which could allow an attacker to escape the Java sandbox and conduct unauthorized activities. Published Before: 1/9/2001 Severity: Medium

CVE-2001-0126: Oracle XSQL servlet 1.0.3.0 and earlier allows remote attackers to execute arbitrary Java code by redirecting the XSQL server to another source via the xml-stylesheet parameter in the xslt stylesheet. Published Before: 3/12/2001 Severity: High

CVE-2001-0137: Windows Media Player 7 allows remote attackers to execute malicious Java applets in Internet Explorer clients by enclosing the applet in a skin file named skin.wmz, then referencing that skin in the codebase parameter to an applet tag. Published Before: 3/12/2001 Severity: High

Category 23.1 Java

2002-12-13 critical flaws Windows operating systems alert Java virtual machine HTML

#### NewsScan

#### MICROSOFT WARNS OF 'CRITICAL' SECURITY FLAWS IN WINDOWS

Microsoft revealed "critical" flaws in its Windows operating system that conceivably could allow hackers to alter data stored in computers, load and run malicious programs, or reformat hard drives. Microsoft is urging Windows users to download a new version of Microsoft Virtual Machine, which is the part of Windows that runs Java applications. "An attacker could, in the most serious of these vulnerabilities, gain complete control of a user's system and take any action" he or she chooses, said John Montgomery, head of Microsoft's developer platform and evangelism group. Security features in Outlook Express 6 and Outlook 2002 are safe from the HTML-mail-based attacks by default and Outlook 98 and 2000 users are also protected if users have installed the Microsoft security updates for them. The good news is, a hacker would have to be quite sophisticated to carry out an attack of the kind described, says Gary Bahadur, CIO at Foundstone. "This is not an easy attack at all. You've got to be pretty slick, pretty creative." (Wall Street Journal 13 Dec 2002)

## 23.2 Javascript

Category 23.2 Javascript

2002-03-10 **JavaScript vulnerabilities ICAT CVE** 

ICAT Metabase

The ICAT Metabase < http://icat.nist.gov/icat.cfm > for the Common Vulnerabilities and Exposures (CVE) database reported the following vulnerabilities involving JavaScript for the period from 1 Jan 2001 to 10 Mar 2002:

CAN-2001-0365: Eudora before 5.1 allows a remote attacker to execute arbitrary code, when the 'Use Microsoft Viewer' and 'allow executables in HTML content' options are enabled, via an HTML email message containing Javascript, with ActiveX controls and malicious code within IMG tags. Published Before: 6/27/2001 Severity: High

CAN-2001-0596: Netscape Communicator prior to 4.77 allows a remote attacker to execute arbitrary javascript via specially crafted GIF images. The javascript is embedded in the GIF file as a comment. Published Before: 8/2/2001 Severity: High

CAN-2001-0722: Internet Explorer 5.5 and 6.0 allows remote attackers to read and modify user cookies via Javascript in an about: URL. Published Before: 12/6/2001 Severity: Medium

CAN-2001-0723: Internet Explorer 5.5 and 6.0 allows remote attackers to read and modify user cookies via Javascript, aka the "Second Cookie Handling Vulnerability." Published Before: 11/14/2001 Severity: Medium

CAN-2001-0743: Paging function in O'Reilly WebBoard Pager 4.10 allows remote attackers to cause a denial of service via a message with an escaped 'character followed by JavaScript commands. Published Before: 10/18/2001 Severity: Medium

CAN-2001-0745: Netscape 4.7x allows remote attackers to obtain sensitive information such as the user's login, mailbox location and installation path via Javascript that accesses the mailbox: URL in the document.referrer property. Published Before: 10/18/2001 Severity: Medium

CAN-2001-0824: Cross-site scripting vulnerability in IBM WebSphere 3.02 and 3.5 FP2 allows remote attackers to execute Javascript by inserting the Javascript into (1) a request for a JSP file, or (2) a request to the webapp/examples/ directory, which inserts the Javascript into an error page. Published Before: 12/6/2001 Severity: High

CAN-2001-0828: A cross-site scripting vulnerability in Caucho Technology Resin before 1.2.4 allows a malicious webmaster to embed Javascript in a hyperlink that ends in a .jsp extension, which causes an error message that does not properly quote the Javascript. Published Before: 12/6/2001 Severity: High

CAN-2001-0829: A cross-site scripting vulnerability in Apache Tomcat 3.2.1 allows a malicious webmaster to embed Javascript in a request for a .JSP file, which causes the Javascript to be inserted into an error message. Published Before: 12/6/2001 Severity: High

CAN-2001-0898: Opera 6.0 and earlier allows remote attackers to access sensitive information such as cookies and links for other domains via Javascript. Published Before: 11/15/2001 Severity: Medium

CAN-2001-0919: Internet Explorer 5.50.4134.0100 on Windows ME with "Prompt to allow cookies to be stored on your machine" enabled does not warn a user when a cookie is set using Javascript, Published Before: 11/26/2001 Severity: High

CAN-2001-0987: Cross-site scripting vulnerability in CGIWrap before 3.7 allows remote attackers to execute arbitrary Javascript on other web clients by causing the Javascript to be inserted into error messages that are generated by CGIWrap. Published Before: 7/22/2001 Severity: High

CVE-2001-0148: The WMP ActiveX Control in Windows Media Player 7 allows remote attackers to execute commands in Internet Explorer via javascript URLs, a variant of the "Frame Domain Verification" vulnerability. Published Before: 6/2/2001 Severity: High

CVE-2001-0149: Windows Scripting Host in Internet Explorer 5.5 and earlier allows remote attackers to read arbitrary files via the GetObject Javascript function and the htmlfile ActiveX object. Published Before: 6/2/2001 Severity: High

### 23.3 ActiveX

Category 23.3 ActiveX

2002-03-10 ActiveX vulnerabilities ICAT CVE

ICAT Metabase

The ICAT Metabase < http://icat.nist.gov/icat.cfm > for the Common Vulnerabilities and Exposures (CVE) database reported the following vulnerabilities involving ActiveX for the period from 1 Jan 2001 to 10 Mar 2002:

CAN-2000-1105: The ixsso query ActiveX Object is marked as safe for scripting, which allows malicious web site operators to embed a script that remotely determines the existence of files on visiting Windows 2000 systems that have Indexing Services enabled. Published Before: 1/9/2001 Severity: Medium

CAN-2001-0365: Eudora before 5.1 allows a remote attacker to execute arbitrary code, when the 'Use Microsoft Viewer' and 'allow executables in HTML content' options are enabled, via an HTML email message containing Javascript, with ActiveX controls and malicious code within IMG tags. Published Before: 6/27/2001 Severity: High

CAN-2001-0538: Microsoft Outlook View ActiveX Control in Microsoft Outlook 2002 and earlier allows remote attackers to execute arbitrary commands via a malicious HTML e-mail message or web page. Published Before: 8/14/2001 Severity: High

CAN-2002-0022: Buffer overflow in the implementation of an HTML directive in mshtml.dll in Internet Explorer 5.5 and 6.0 allows remote attackers to execute arbitrary code via a web page that specifies embedded ActiveX controls in a way that causes 2 Unicode strings to be concatenated. Published Before: 3/8/2002 Severity: High

CVE-2001-0090: The Print Templates feature in Internet Explorer 5.5 executes arbitrary custom print templates without prompting the user, which could allow an attacker to execute arbitrary ActiveX controls, aka the "Browser Print Template" vulnerability. Published Before: 2/16/2001 Severity: High

CVE-2001-0091: The ActiveX control for invoking a scriptlet in Internet Explorer 5.0 through 5.5 renders arbitrary file types instead of HTML, which allows an attacker to read arbitrary files, aka a variant of the "Scriptlet Rendering" vulnerability. Published Before: 2/16/2001 Severity: Medium

CVE-2001-0148: The WMP ActiveX Control in Windows Media Player 7 allows remote attackers to execute commands in Internet Explorer via javascript URLs, a variant of the "Frame Domain Verification" vulnerability. Published Before: 6/2/2001 Severity: High

CVE-2001-0149: Windows Scripting Host in Internet Explorer 5.5 and earlier allows remote attackers to read arbitrary files via the GetObject Javascript function and the htmlfile ActiveX object. Published Before: 6/2/2001 Severity: High

CVE-2001-0434: The LogDataListToFile ActiveX function used in (1) Knowledge Center and (2) Back web components of Compaq Presario computers allows remote attackers to modify arbitrary files and cause a denial of service. Published Before: 7/2/2001 Severity: High

### 23.4 HTML, XML

Category 23.4 HTML, XML

2002-01-10 SSL https padlock icon misleading interpretation programming

RISKS 21 86ff

A discussion in RISKS led to some interesting analysis of the disconnect between the state of the padlock icon on Web browsers and the use of SSL. The problem began with a visit to the Kaiser Permanent Web site for members at < http://www.kponline.org/ >. All attempts to initiate https connections appeared to fail. However, in a followup, Geoff Kuenning summarized the situation neatly as follows:

>... [I]n viewing the source of the referenced Web page, it appears that the "sign on" button makes an https (SSL) connection. Thus, although the "padlock" icon in the browser is unlocked, anything sent from that page is in fact sent using SSL.

I have recommended that Kaiser change their main page so that it forwards the browser to an SSL equivalent, solely so that the padlock icon will appear locked.

I think that the true RISK is not in Kaiser's Web page, but rather in the browser. The "padlock" icon reflects not whether the page SENDS information securely, but rather the fact that the page was FETCHED securely. This disconnect between what is shown and what is expected has been raised recently by Jeff Mogul in the converse direction: a page that had the padlock proceeded to send information insecurely.

The first problem (apparently insecure page is actually secure) can be patched around with the forwarding kludge I mentioned above. The second can be handled by the user to some extent (certain browser settings can warn you when you transition from a secure page to an insecure one). However, the true problem is in browser design. The "padlock" icon should be associated with a LINK, not a page. Regardless of how it was fetched, if a page contains both secure and insecure links, the lock should be shown as unlocked and should lock only when you mouse over a secure link. Only if all outgoing links from a page are secure should the padlock be permanently displayed in its locked form.

MORAL: It is not enough to be secure; you must be SEEN to be secure.

Category 23.4 HTML, XML

2002-01-28 Web page hijacking URL user ID misleading trickery dissimulation spoofing

browser

RISKS 21 89

Rob Graham spotted a dangerous application of syntax in a URL that looked like this:

< http://www.microsoft.com&item=3Dq209354@hardware.no/nyheter/feb01/Q209354 %20%20HOWTO.htm >

The naïve users would assume that the URL is part of the microsoft.com domain; in fact, this syntax means that a user ID and password (the part in front of the @ sign) is being passed to the URL \_following\_ the @ sign.

[MK notes: In testing this in March 2002 using MS IE6, I was taken directly to the "hardware.no" site, where a message read "This page has been removed after request from Microsoft...." In contrast, using my preferred browser, Opera 6.01, I received a pop-up warning from the browser alerting me to the fact that the string "www.microsoft.com&item=3Dq209354" was in fact a user ID and password and asking if it was OK to proceed. Bravo Opera!]

Category 23.4 HTML, XML

2002-03-10 HTML vulnerabilities ICAT CVE

ICAT Metabase

The ICAT Metabase < http://icat.nist.gov/icat.cfm > for the Common Vulnerabilities and Exposures (CVE) database reported the following vulnerabilities involving ActiveX for the period from 1 Jan 2001 to 10 Mar 2002:

CAN-2000-0898: Small HTTP Server 2.01 does not properly process Server Side Includes (SSI) tags that contain null values, which allows local users, and possibly remote attackers, to cause the server to crash by inserting the SSI into an HTML file. Published Before: 1/9/2001 Severity: Medium

CAN-2000-1172: Buffer overflow in Gaim 0.10.3 and earlier using the OSCAR protocol allows remote attackers to conduct a denial of service and possibly execute arbitrary commands via a long HTML tag. Published Before: 1/9/2001 Severity: High

CAN-2001-0322: MSHTML.DLL HTML parser in Internet Explorer 4.0, and other versions, allows remote attackers to cause a denial of service (application crash) via a script that creates and deletes an object that is associated with the browser window object. Published Before: 6/2/2001 Severity: Medium

CAN-2001-0365: Eudora before 5.1 allows a remote attacker to execute arbitrary code, when the 'Use Microsoft Viewer' and 'allow executables in HTML content' options are enabled, via an HTML email message containing Javascript, with ActiveX controls and malicious code within IMG tags. Published Before: 6/27/2001 Severity: High

CAN-2001-0389: IBM Websphere/NetCommerce3 3.1.2 allows remote attackers to determine the real path of the server by directly calling the macro.d2w macro with a NOEXISTINGHTMLBLOCK argument. Published Before: 7/2/2001 Severity: Medium

CAN-2001-0484: Tektronix PhaserLink 850 does not require authentication for access to configuration pages such as \_ncl\_subjects.shtml and \_ncl\_items.shtml, which allows remote attackers to modify configuration information and cause a denial of service by accessing the pages. Published Before: 6/27/2001 Severity: Medium

CAN-2001-0519: Aladdin eSafe Gateway versions 2.x allows a remote attacker to circumvent HTML SCRIPT filtering via a special arrangement of HTML tags which includes SCRIPT tags embedded within other SCRIPT tags. Published Before: 8/14/2001 Severity: Medium

CAN-2001-0520: Aladdin eSafe Gateway versions 3.0 and earlier allows a remote attacker to circumvent filtering of SCRIPT tags by embedding the scripts within certain HTML tags including (1) onload in the BODY tag, (2) href in the A tag, (3) the BUTTON tag, (4) the INPUT tag, or (5) any other tag in which scripts can be defined. Published Before: 8/14/2001 Severity: Medium

CAN-2001-0521: Aladdin eSafe Gateway versions 3.0 and earlier allows a remote attacker to circumvent HTML SCRIPT filtering via the UNICODE encoding of SCRIPT tags within the HTML document. Published Before: 8/14/2001 Severity: Medium

CAN-2001-0523: eEye SecureIIS versions 1.0.3 and earlier allows a remote attacker to bypass filtering of requests made to SecureIIS via the escaping of HTML characters within the request, which could allow a remote attacker to use restricted variables and perform directory traversal attacks on vulnerable programs that would otherwise be protected by SecureIIS. Published Before: 8/14/2001 Severity: Medium

CAN-2001-0538: Microsoft Outlook View ActiveX Control in Microsoft Outlook 2002 and earlier allows remote attackers to execute arbitrary commands via a malicious HTML e-mail message or web page. Published Before: 8/14/2001 Severity: High

CAN-2001-0726: Outlook Web Access (OWA) in Microsoft Exchange 5.5 Server, when used with Internet Explorer, does not properly detect certain inline script, which can allow remote attackers to perform arbitrary actions on a user's Exchange mailbox via an HTML e-mail message. Published Before: 12/6/2001 Severity: High

CAN-2001-0835: Cross-site scripting vulnerability in Webalizer 2.01-06, and possibly other versions, allows remote attackers to inject arbitrary HTML tags by specifying them in (1) search keywords embedded in HTTP referrer information, or (2) host names that are retrieved via a reverse DNS lookup. Published Before: 12/6/2001 Severity: High

CAN-2001-0837: DeltaThree Pc-To-Phone 3.0.3 places sensitive data in world-readable locations in the installation directory, which allows local users to read the information in (1) temp.html, (2) the log folder, and (3) the PhoneBook folder. Published Before: 12/6/2001 Severity: Medium

CAN-2001-0874: Internet Explorer 5.5 and 6.0 allow remote attackers to read certain files via HTML that passes information from a frame in the client's domain to a frame in the web site's domain, a variant of the "Frame Domain Verification" vulnerability. Published Before: 12/13/2001 Severity: Medium

CAN-2001-0901: Hypermail allows remote attackers to execute arbitrary commands on a server supporting SSI via an attachment with a .shtml extension, which is archived on the server and can then be executed by requesting the URL for the attachment. Published Before: 11/19/2001 Severity: High

CAN-2001-0925: The default installation of Apache before 1.3.19 allows remote attackers to list directories instead of the multiview index.html file via an HTTP request for a path that contains many / (slash) characters, which causes the path to be mishandled by (1) mod\_negotiation, (2) mod\_dir, or (3) mod\_autoindex. Published Before: 3/12/2001 Severity: Medium

CAN-2001-0948: Cross-site scripting (CSS) vulnerability in ValiCert Enterprise Validation Authority (EVA) 3.3 through 4.2.1 allows remote attackers to execute arbitrary code or display false information by including HTML or script in the certificate's description, which is executed when the certificate is viewed. Published Before: 12/4/2001 Severity: High

CAN-2001-1013: Apache on Red Hat Linux with with the UserDir directive enabled generates different error codes when a username exists and there is no public\_html directory and when the username does not exist, which could allow remote attackers to determine valid usernames on the server. Published Before: 9/12/2001 Severity: Medium

CAN-2001-1019: Directory traversal vulnerability in view\_item CGI program in sglMerchant 1.0 allows remote attackers to read arbitrary files via a .. (dot dot) in the HTML\_FILE parameter. Published Before: 9/8/2001 Severity: Medium

CAN-2002-0022: Buffer overflow in the implementation of an HTML directive in mshtml.dll in Internet Explorer 5.5 and 6.0 allows remote attackers to execute arbitrary code via a web page that specifies embedded ActiveX controls in a way that causes 2 Unicode strings to be concatenated. Published Before: 3/8/2002 Severity: High

CAN-2002-0024: File Download box in Internet Explorer 5.01, 5.5 and 6.0 allows an attacker to use the Content-Disposition and Content-Type HTML header fields to modify how the name of the file is displayed, which could trick a user into believing that a file is safe to download. Published Before: 3/8/2002 Severity: High

CAN-2002-0025: Internet Explorer 5.01, 5.5 and 6.0 does not properly handle the Content-Type HTML header field, which allows remote attackers to modify which application is used to process a document. Published Before: 3/8/2002 Severity: Medium

CVE-2000-0897: Small HTTP Server 2.01 allows remote attackers to cause a denial of service by repeatedly requesting a URL that references a directory that does not contain an index.html file, which consumes memory that is not released after the request is completed. Published Before: 1/9/2001 Severity: Medium

CVE-2000-1187: Buffer overflow in the HTML parser for Netscape 4.75 and earlier allows remote attackers to execute arbitrary commands via a long password value in a form field. Published Before: 1/9/2001 Severity: High

CVE-2001-0002: Internet Explorer 5.5 and earlier allows remote attackers to obtain the physical location of cached content and open the content in the Local Computer Zone, then use compiled HTML help (.chm) files to execute arbitrary programs. Published Before: 7/21/2001 Severity: High

CVE-2001-0028: Buffer overflow in the HTML parsing code in oops WWW proxy server 1.5.2 and earlier allows remote attackers to execute arbitrary commands via a large number of " (quotation) characters. Published Before: 2/12/2001 Severity: High

CVE-2001-0089: Internet Explorer 5.0 through 5.5 allows remote attackers to read arbitrary files from the client via the INPUT TYPE element in an HTML form, aka the "File Upload via Form" vulnerability. Published Before: 2/16/2001 Severity:

CVE-2001-0091: The ActiveX control for invoking a scriptlet in Internet Explorer 5.0 through 5.5 renders arbitrary file types instead of HTML, which allows an attacker to read arbitrary files, aka a variant of the "Scriptlet Rendering" vulnerability. Published Before: 2/16/2001 Severity: Medium

CVE-2001-0130: Buffer overflow in HTML parser of the Lotus R5 Domino Server before 5.06, and Domino Client before 5.05, allows remote attackers to cause a denial of service and possibly execute arbitrary commands via a malformed font size specifier. Published Before: 3/12/2001 Severity: High

CVE-2001-0149: Windows Scripting Host in Internet Explorer 5.5 and earlier allows remote attackers to read arbitrary files via the GetObject Javascript function and the htmlfile ActiveX object. Published Before: 6/2/2001 Severity: High

CVE-2001-0154: HTML e-mail feature in Internet Explorer 5.5 and earlier allows attackers to execute attachments by setting an unusual MIME type for the attachment, which Internet Explorer does not process correctly. Published Before: 5/3/2001 Severity: Medium

CVE-2001-0243: Windows Media Player 7 and earlier stores Internet shortcuts in a user's Temporary Files folder with a fixed

filename instead of in the Internet Explorer cache, which causes the HTML in those shortcuts to run in the Local Computer Zone instead of the Internet Zone, which allows remote attackers to read certain files. Published Before: 6/27/2001 Severity: Medium

CVE-2001-0340: An interaction between the Outlook Web Access (OWA) service in Microsoft Exchange 2000 Server and Internet Explorer allows attackers to execute malicious script code against a user's mailbox via a message attachment that contains HTML code, which is executed automatically. Published Before: 7/21/2001 Severity: High

CVE-2001-0457: man2html before 1.5-22 allows remote attackers to cause a denial of service (memory exhaustion). Published Before: 6/27/2001 Severity: Medium

Category 23.4 HTML, XML

2002-04-22 HTLM vulnerability arbitrary code denial-of-service attack DoS kernel panic crash Macintosh

RISKS, http://news.com.com/2100-1001-884364.html

22 04

Robert Lemos wrote in CNET News:

Microsoft acknowledged on Tuesday that its popular Office applications for the Macintosh have a critical security flaw that leaves users' systems open to attack by worms and online vandals. The software slip-up happens because the Microsoft applications incorrectly handle the input to a certain HTML (Hypertext Markup Language) feature. By formatting a link in a particular manner, an attacker can cause a program to crash a Macintosh or run arbitrary commands. The link could appear on a Web page or in an HTML-enabled e-mail. [...] http://news.com.com/2100-1001-884364.html

Category 23.4 HTML, XML

2002-06-10 Excel spreadsheet vulnerability arbitrary code XML

RISKS 22 12

Patrick O'Beirne contributed this item to RISKS:

>A security hole in Excel XP spreadsheets which could lead to a hack attack has been exposed. The discovery was made by independent security expert Georgi Guninski, who said on his Web site: "Excel XP tries to play with new technologies like XML and XSLT. Unfortunately the Excel seem so flawed that if the user opens a .xls file and chooses to view it with xml stylesheet arbitrary code may be executed. As script kiddies know this may lead to taking full control over a user's computer." Guninski, who has posted a sample of the code in his site, said users should not use XML stylesheets.<

Category 23.4 HTML, XML

2002-07-16 content filter substitution replacement Web site corruption criminal hackers cross-site scripting HTML

#### NewsScan

#### THE NEW LANGUAGE OF THE WEB

An e-mail security filter used by Yahoo has spawned a bizarre revision of the text in hundreds of Web sites by deleting letter combinations that could be used by hackers and replacing them with innocuous words. For example, "eval" has been converted to "review", so that the word "medieval" now appears as "medireview" on many sites. A recent search conducted by British Internet site NTK found that 640 different Web sites now contain the word "medieveiew" in place of "medieval." The offending words, which also include "mocha" (changed to "espresso") and "expression" (replaced by "statement"), are blacklisted because they could be used for cross-site scripting -- embedding potentially dangerous code into a Web page or an e-mail message written in HTML. (New Scientist 15 Jul 2002)

http://www.newscientist.com/news/news.jsp?id=ns99992546

Category 23.4 HTML, XML

2002-12-23 pop-up advertising Web hijacking HTML

NewsScan

#### POP-UP ADS 'KICK THROUGH'

Pop-up ads are becoming increasingly annoying, and the latest twist will make it harder for Web users to simply ignore them. A new technique called "kick through" enables advertisers to direct a person to another Web site if they simply move their cursor across the ad -- no clicking is necessary. Many people are complaining that the new ads are overstepping the boundaries of an already intrusive form of online advertising. "When I tried to close the window it kicked me to the site, which is really annoying when I have six windows open and three of which were not by my own doing," says one irate victim. Orbitz, which appears to be the only advertiser currently using the kick through, defends its strategy: "The enormous success for Orbitz is directly related to these pop-unders. There's an enormous segment of the population that are appreciating these ads," says Mark Rattin, creative director for Otherwise, which devised the ads for Orbitz. He says there's only a 30% chance that viewers will be kicked through to the Orbitz site by rolling over the ads. (CNet News.com 20 Dec 2002)

http://news.com.com/2100-1023-978616.html

## 23.5 E-mail & instant messaging or chat

Category 23.5 E-mail & instant messaging or chat

2002-01-04 denial-of-service DoS attack vulnerability servers instant messaging chat

NewsScan

#### AOL FIXES BUG IN INSTANT MESSENGER

AOL Time Warner says it has patched the software on its central servers to fix a problem in the free, downloadable version of the Windows versions of its Instant Messenger (AIM) software that could have allowed a network vandal to flood a victim's computer with data. (San Jose Mercury News 4 Jan 2002)

http://www.siliconvalley.com/docs/news/svfront/aol010402.htm

Category 23.5 E-mail & instant messaging or chat

2002-03-10 e-mail chat vulnerabilities ICAT CVE

#### ICAT Metabase

The ICAT Metabase < http://icat.nist.gov/icat.cfm > for the Common Vulnerabilities and Exposures (CVE) database reported the following vulnerabilities involving e-mail or chat for the period from 1 Jan 2001 to 10 Mar 2002:

CAN-2001-0581: Spytech Spynet Chat Server 6.5 allows a remote attacker to create a denial of service (crash) via a large amount (> 100) of connections to port 6387. Published Before: 8/22/2001 Severity: Medium

CAN-2001-0615: Directory traversal vulnerability in Faust Informatics Freestyle Chat server prior to 4.1 SR3 allows a remote attacker to read arbitrary files via a specially crafted URL which includes variations of a '..' (dot dot) attack such as '...' or '....'. Published Before: 8/14/2001 Severity: Medium

CAN-2001-0616: Faust Informatics Freestyle Chat server prior to 4.1 SR3 allows a remote attacker to create a denial of service via a URL request which includes a MS-DOS device name (e.g., GET /aux HTTP/1.0). Published Before: 8/14/2001 Severity: Medium

CAN-2001-0726: Outlook Web Access (OWA) in Microsoft Exchange 5.5 Server, when used with Internet Explorer, does not properly detect certain inline script, which can allow remote attackers to perform arbitrary actions on a user's Exchange mailbox via an HTML e-mail message. Published Before: 12/6/2001 Severity: High

CAN-2001-0792: Format string vulnerability in XChat 1.2.x allows remote attackers to execute arbitrary code via a malformed nickname. Published Before: 10/18/2001 Severity: High

CAN-2001-0857: Cross-site scripting vulnerability in status.php3 in Imp Webmail 2.2.6 and earlier allows remote attackers to gain access to the e-mail of other users by hijacking session cookies via the message parameter. Published Before: 12/6/2001 Severity: Medium

CAN-2001-0945: Buffer overflow in Outlook Express 5.0 through 5.02 for Macintosh allows remote attackers to cause a denial of service via an e-mail message that contains a long line. Published Before: 12/3/2001 Severity: Medium

CVE-2000-1148: The installation of VolanoChatPro chat server sets world-readable permissions for its configuration file and stores the server administrator passwords in plaintext, which allows local users to gain privileges on the server. Published Before: 1/9/2001 Severity: Medium

CVE-2001-0154: HTML e-mail feature in Internet Explorer 5.5 and earlier allows attackers to execute attachments by setting an unusual MIME type for the attachment, which Internet Explorer does not process correctly. Published Before: 5/3/2001 Severity: Medium

Category 23.5 E-mail & instant messaging or chat

2002-03-11 cellular phones wireless virus worm malware palmtop

NewsScan

#### FOR VANDALS, SMART PHONES NEW AND INVITING TARGETS

Stephen Trilling, research at Symantec, which makes antivirus software, warns: "We should think of smart phones as just another set of computers on the Internet. If they're connected to the Internet they can be used to transmit threats and attack targets, just as any computer can. It's technically possible right now." Recently, several software companies have begun selling antivirus and encryption software for smartphone operating systems made by Palm, Microsoft and the Symbian platform common in Europe. Ari Hypponen enumerates some of the dangers: "If a malicious piece of code gets control of your phone, it can do everything you can do. It can call toll numbers. It can get your messages and send them elsewhere. It can record your passwords." And he adds that it's not that hard to do: "It's possible for anyone to make custom software for this platform. Teens can download development tools and write their own software." (San Jose Mercury News 10 Mar 2002) http://www.siliconvalley.com/mld/siliconvalley/2833740.htm

Category 23.5 E-mail & instant messaging or chat

2002-05-08 anti-malware e-mail worm virus moderated mailing list design standards

RISKS 22 06

Mailing list management software often uses a coded REPLY-TO address so that the moderator can simply REPLY to a proposed posting and send it to the entire list. Unfortunately, an anti-virus running on the moderator's workstation does the same when it encounters a virus-infested submission, thus sending the infection out to the entire list without letting the moderator stop it.

In a followup piece, a RISKS contributor noted that the design error is the anti-virus package's use of the REPLY-TO field rather than the RETURN-PATH address. In other words, the sender of the message should be informed that it is virus infected; the recipient of replies may be very different from the sender, as in this case.

Category 23.5 E-mail & instant messaging or chat

2002-05-10 instant messenger online chat quality assurance QA

NewsScan

#### SOFTWARE WILL HAVE FLAWS

Microsoft says that the latest versions of its MSN Messenger program contain a "critical" flaw that a hacker could exploit for malicious purposes. At issue is a feature that allows users to congregate in a virtual "chat room" to exchange messages . A Microsoft executive says: "Software always will have flaws. We always do our best to ensure we do not have flaws or vulnerabilities, but while we strive for perfection, we know we're not always going to achieve perfection." (AP/USA Today 9 May 2002)

http://www.usatoday.com/life/cyber/tech/2002/05/09/messenger-flaw.htm

Category 23.5 E-mail & instant messaging or chat

2002-05-27 HTML control command language e-mail

RISKS 22 10

In a newsletter sent to 40,000 recipients, I included a block of HTML code showing a forged header.

The e-mail list software spotted what it thought was the end of the document and inserted the e-mail address of each recipient in that person's copy of the newsletter, making many readers believe that their e-mail address had been distributed to the entire list. Result: hundreds of letters (some nice, some not).

#### LESSONS:

- (1) When designing macros that scan for search strings associated with a particular condition (in this case, the end of a message), it would be wise to test the presumption that the condition is in fact true. In this example, perhaps a second check might verify that there is in fact no further text in the message before inserting the valediction.
- (2) When quoting control language (in this case, HTML), and in the absence of some sort of escape character (meaning "the following is literal text, not command language"), we may avoid accidents by using symbol substitution to prevent accidental misreading of the quoted strings as if they were actually to be interpreted.

Category 23.5 E-mail & instant messaging or chat

2002-05-29 instant messaging chat vulnerabilities tunneling

NewsScan

#### INSTANT MESSAGING CAN OPEN CORPORATE NETS TO VANDALISM

AOL and Microsoft freely admit that their popular instant messaging systems were designed for chat and not for transmission of sensitive corporate messages, but they are now building secure IM services for use by large customer groups. Why? Because, according to research firm IDC, 54 million employees this year will be using consumer IM systems for work-related purposes. Until they're using more secure instant messaging systems, companies need to be careful of what they do. Security expert Dan Ingevaldson of Internet Security Systems says that free IM systems represent a "huge gaping security risk for companies." (USA Today 28 May 2002)

http://www.usatoday.com/life/cyber/tech/2002/05/29/im-security.htm

E-mail & instant messaging or chat Category 23.5

2002-09-04 instant messaging surveillance workplace communication standards policies

telecommuting

#### NewsScan

#### INSTANT MESSAGING A HIT IN CORPORATE WORLD

Businesses with multiple office locations increasingly are finding that instant messaging can provide the real-time connectivity missing in e-mail and voice-mail exchanges. The beauty of IM, as it's called, is not only that it catches the recipient's attention immediately by popping up on his or her screen, but it also tells the sender which recipients are available to communicate at that moment. IM is "absolutely useful in trying to figure out, 'Can I get to this person?'" says a Lehman Brothers managing director. Fans say it's reversing a 20-year trend toward employee insulation, with voice-mail systems that make it difficult to tell whether workers are in the office or out on the golf course. Advocates also note that IM has influenced managers to be more receptive to telecommuting arrangements, because it can verify who is really working from home, or at least is logged onto the computer there. And because failing to answer an IM quickly is considered rude, most workers use the "away from my desk" or "busy" sign when they're absent. "There's a sensation you can't hide," says one long-distance manager. IDC estimates that by the end of last year, 20 million people worldwide were using IM in businesses, and it predicts that number will soar to 300 million by the end of 2005. (Wall Street Journal 4 Sep 2002)

E-mail & instant messaging or chat Category 23.5

2002-10-07 instant messaging corporate monitoring security encryption authentication

NewsScan

#### YAHOO TARGETS BUSINESS WITH CORPORATE IM SERVICE

Yahoo is launching a test version of a new instant-messaging service for business users in the next few months in another bid to diversify its revenue stream beyond advertising. When it's formally launched in early 2003, the Yahoo Messenger Enterprise Edition 1.0 will cost \$30 per user per year, which includes software upgrades and support. Yahoo plans to differentiate its corporate IM service by adding security, administrative control and integration features, enabling companies to audit incoming and outgoing messages, as well as add encryption and authenticate users. Competitors Microsoft and AOL are believed to be preparing their own corporate messaging services, and analysts say Yahoo must move quickly to build its customer base and retain loyal users who might be tempted to migrate to rival services. (Wall Street Journal 7 Oct 2002)

Category 23.5 E-mail & instant messaging or chat

2002-12-05 securities industry SEC regulations record-keeping rules fines archives e-mail

retention

#### NewsScan

#### FIRMS FINED FOR NOT FOLLOWING E-MAIL RETENTION SCHEDULE

The Securities and Exchange Commission has fined five major brokerage firms (Deutsche Bank, Goldman Sachs, Morgan Stanley, Salomon Smith Barney, and U.S. Bancorp Piper Jaffray) \$1.65 million each for failing to keep employee e-mail for the required retention period. The SEC examines such mail to find cases in which brokers have rated stocks positively and given it a "buy" recommendation to the public, while in private correspondence revealed complete contempt for the same stock. The commission says, "The record-keeping rules are a keystone of the surveillance of brokers and dealers by commission staff and the security industry's self-regulatory bodies." (San Jose Mercury News 4 Dec 2002)

http://www.siliconvalley.com/mld/siliconvalley/4661957.htm

# 23.6 Web-site infrastructure, general Web security issues

Category 23.6 Web-site infrastructure, general Web security issues

2002-01-07 Web site design ActiveX operating system compatibility standards security

RISKS 21 86

Koos van den Hout noted in RISKS that the mcafee.com Web site "shows a pop-up asking me to enable an ActiveX plug-in...

The fact that I am using a different operating system for which an ActiveX plug-in isn't available at all has never crossed the mind of whoever designed that." As he continued his browsing, he found that when he used the text-based Lynx 2.8.2 browser for Unix, he was told to lower the security setting for his browser -- in terms clearly indicating that the designer was taking MS Internet Explorer for granted.

Category 23.6 Web-site infrastructure, general Web security issues

2002-01-10 confidentiality SSL https implementation failure URL QA quality assurance

RISKS 21 86

Skip La Fetra pointed out in RISKS that some Web sites boasting of SSL and HTTPS connections construct URLs that contain sensitive details of a transaction. In his example, one page constructed a URL

"https://securesite.com/verification.htm?name=3Dyyyyyy,CardNumber=3D12345=6789,ExpirationDate=3D12/31/2001" which Being part of the URL "address", this information included his name, address, credit card number, and expiration date. Such URLs \_can\_ be intercepted and the information abused despite the encryption of the page contents.

Category 23.6 Web-site infrastructure, general Web security issues

2002-01-10 SSL https e-mail insecure transmission privacy design

RISKS 21 86

J. Debert noted an inconsistency in attempts to protect consumer privacy:

>ATT allows customers to send form mail using SSL on their Web site. This is to keep their customer's info and the message private.

But their people include the entire message in plaintext e-mail messages sent in response defeating the purpose of the secure form.

Category 23.6 Web-site infrastructure, general Web security issues

2002-02-11 credit card Internet security risks bank failure government regulators

NewsScan; http://www.usatoday.com/life/cyber/tech/2002/02/08/nextbank.htm

NEXTBANK BECOMES FIRST INTERNET BANK TO FAIL

Federal regulators have shut down Phoenix-based NextBank, whose principal business was issuing credit cards over the Internet. The government's Office of the Comptroller of the Currency said that NextBank's "unsafe and unsound practices" (making loans to poor-credit customers who were unable to handle payments) made it unlikely that the bank would be able "to pay its obligations in the normal course of business" without federal assistance. The Federal Deposit Insurance Corporation (FDIC) will begin mailing checks today to the bank's customers for the amount of their insured deposits. (AP/USA Today 8 Feb 2002)

Web-site infrastructure, general Web security issues Category 23.6

2002-02-13 vulnerability remote control shutdown penetration

NewsScan; CERT® Advisory CA-2002-03 http://www.cert.org/advisories/CA-2002-03.html

## SECURITY EXPERTS ISSUE WARNING [13 Feb 2002]

CERT/CC, a center of Internet security expertise, at the Software Engineering Institute, a federally funded research and development center operated by Carnegie Mellon University, is warning computer users of a network security flaw that could allow a computer to be invaded remotely by vandals who could take over and shut down the system. Shawn Herman of CERT says that virtually every network uses a multitude of devices that may have the security flaw. To see a list of potential vulnerabilities and what to do about them, go to

http://www.cert.org/. (New York Times 13 Feb 2002)

http://partners.nytimes.com/2002/02/13/technology/13NET.html

Web-site infrastructure, general Web security issues Category 23.6 2002-03-10 Web server vulnerabilities ICAT CVE

#### ICAT Metabase

The ICAT Metabase < http://icat.nist.gov/icat.cfm > for the Common Vulnerabilities and Exposures (CVE) database reported 76 vulnerabilities involving Web servers out of a total of 1241 for the period from 1 Jan 2001 to 10 Mar 2002. This represents about 6% of all vulnerabilities logged for that period. Overall, for the entire period since the CVE began recording vulnerabilities in 1995, Web servers are named in 199 of the 3677 vulnerabilities or about 5% of the total.

Category 23.6 Web-site infrastructure, general Web security issues

2002-03-11 quality assurance QA Web design I&A identification authentication password

failure flaw goofball idiots fools stupidity absurd

RISKS 21 94

Grant Bayley reported that in Australia, an error in the programming for the Web-based registration system for names in the .org.au, .gov.au, and .edu.au domains allowed anyone to change ownership details of any domain instantly without even knowing the right password. Such a hole would have allowed complete hijacking of every non-commercial domain in Australia, including police forces and state governments.

Web-site infrastructure, general Web security issues Category 23.6

2002-03-14 design QA quality assurance Web URL discounts confidentiality

RISKS 01

Saab USA sent out a promotion offering discounts to people who used a Web site with unique URLs for each recipient. Unfortunately, the URLs used sequential ID numbers. Entering a randomly-generated URL resulted in access to the name and address of some other recipient of the offer. In addition, there was nothing to stop users from printing more than one of the supposedly mutual discount offers available on the Web site, thus resulting in more discounts than the company apparently intended to offer. When Ron Gut, who reported on this case to RISKS, tried to use Saab's contact form to suggest improvements, he discovered that the form did not work with Netscape v4.7.

Category 23.6 Web-site infrastructure, general Web security issues

2002-03-27 identity theft confidentiality online auction I&A identification authentication denial of service Web design passwords timeout inactivation lock penetration brute force

dictionary attack password cracking

RISKS, http://zdnet.com.com/2100-1106-868306.html 98 21

E-bay acounts are not protected by any limitation on the number of incorect logons; far from including a lockout, the service does not even impose a timeout. The system is ripe for brute-force, automated password-cracking. According to Scott Nicol, writing in RISKS, e-Bay chose this strategy to preclude denial-of-service attacks that become too easy when an account is locked simply because of repeated bad passwords. [MK notes: This is a classic example of the tradeoffs that different security measures impose: add a delay and you have made the attacker's job easier if their goals is DoS – they just have to send the same wrong password often enough to initiate another timeout. A reasonable approach would be to leave the zero-knowledge approach and look for patterns of attack so that the system can selectively respond to \_attacks\_ and not to \_mistakes\_.]

Category 23.6 Web-site infrastructure, general Web security issues

2002-04-22 vulnerabilities buffer overflow database server arbitrary code

Security Wire Digest 4 31

Shawna McAlearney wrote in Security Wire Digest about an important patch:

>Microsoft last week [mid-April 2002] urged SQL Server users to immediately patch a vulnerability that could allow an attacker to run code of choice on a target machine.

Ranked as a "moderate" threat by Microsoft, the "SQL Extended Procedure Functions Contain Unchecked Buffers" flaw affects SQL Server 7.0/2000. Those versions provide extended stored procedures that fail to validate input correctly, making them susceptible to buffer overflows.

An attacker exploiting the flaw could cause the SQL Server service to fail, or run code in the security context in which SQL Server is running--by default set to domain user. Microsoft says the precise privileges the attacker could gain depend upon the specific security context that the service runs in.

Category 23.6 Web-site infrastructure, general Web security issues

2002-05-05 privacy browser QA quality assurance bugs flaws weaknesses vulnerabilities

exploits demonstrations

RISKS, http://www.newsbytes.com/news/02/176077.html

22 05

Brian McWilliams wrote in Newsbytes:

Security flaws in privacy features added to Microsoft's Web browser could enable attackers to perform several privacy-robbing attacks, including hijacking victims' MSN Messenger accounts, a security researcher warned. According to Thor Larholm, a developer with Denmark-based Internet portal Jubii.dk, "severe" bugs in the "Privacy Report" feature in Internet Explorer version 6 can be exploited "in effect removing all privacy." Last week, Larholm posted an advisory and harmless demonstrations of the flaws at his personal Web site. One example showed how the browser bugs enable a Web site to launch programs that exist on the user's hard disk. Another demo page silently sends a message to users in the target's MSN Messenger contact list....

Category 23.6 Web-site infrastructure, general Web security issues

2002-05-18 Web design failure QA quality assurance SSL HTTPS credit card

RISKS 22 07

VeriSign sells security services such as the "Code Signing Digital ID." However, reported Daniel Norton in RISKS, when you fill out your subscription form on line, the information including your credit-card data is sent in the clear using HTTP instead of HTTPS with SSL.

Category 23.6 Web-site infrastructure, general Web security issues

2002-05-20 cumulatative patch weakness flaws QA quality assurance

Security Wire Digest 4 39

Advisory MS-02-023 caused a fuss because GreyMagic Software complained that the cumulative patch contained major flaws. Shawna McAlearney summarized the situation as follows in Security Wire Digest:

>

**RISKS** 

GreyMagic says Microsoft misunderstood what it called a cross-site scripting problem. "They only patched a symptom of this vulnerability, not its root cause," says GreyMagic. "The problem is not plain cross-site scripting, the problem is that dialogArguments' security restrictions are bypassed and it is passed to the dialog even though it shouldn't be."

GreyMagic now also contends that Microsoft failed to provide a sufficient patch for an earlier flaw.

"MS02-023 also allegedly patches the cssText issue we found back in February, but the patch is weak and can be easily circumvented," says GreyMagic. "So far we have a bulletin full of errors, which was partly fixed by Microsoft; an incomplete patch to the dialogArguments critical vulnerability, leaving IE 5.0 and IE 5.5 exposed; and a useless patch to the cssText vulnerability, leaving all users exposed to (a) critical vulnerability."

Causing further confusion is the "content-disposition: inline" IE flaw discovered by the LAC Corp. that "allows for downloading of a file and its automatic execution under several circumstances without the knowledge of the user."

Microsoft earlier dismissed LAC's advisory as "inaccurate" and having "nothing to do with either Internet Explorer or the security patch" released last year to fix a similar vulnerability, according to a Newsbytes report. MS02-023 acknowledges that IE 5.01/6 are vulnerable to the attack reported by LAC.

Category 23.6 Web-site infrastructure, general Web security issues

2002-05-23 fraud loop lockout availability Web design priority I&A identification authentication child protection credit card

22

Daniel P. B. Smith presented an interesting case of bad design in his submission to RISKS. He needed to change the privacy settings on his Microsoft Passport account and, while he was at it, he had the idea of altering his name and age on the Web form presented for editing his profile. Unfortunately, he changed his name to Mickey Mouse and claimed he was born on 2001-04-01. This false entry then immediately locked him out of the profile editor because "he" was under 13! The only way to change the record was to create a new account that would allow him to alter the records for his "child." [MK comments: Personally, I don't like the idea of supplying false information to \_anyone\_. If you don't agree to the terms of a contract, don't accept the contract. The other message I glean from this case is that when you design a fail-safe mechanism, don't convert a process or account from a higher priority to a lower priority without confirming that the change is correct. In this case, a message informing the user, "If you change the birthday to indicate that you are less than 13 years old, you will lose the ability to update your profile" could have prevented the problem.]

Category 23.6 Web-site infrastructure, general Web security issues

2002-06-18 MS IIS alert vulnerability Web server flaw bug weakness patch

FindLaw Download This 90

#### MICROSOFT DISCLOSES SOFTWARE FLAW

Microsoft Corp. acknowledged a serious flaw Wednesday in its Internet server software that could allow sophisticated hackers to seize control of Web sites, steal information and use vulnerable computers to attack others online. The software, which runs about one-third of the world's Web sites, is used by millions of businesses and organizations but less commonly by home users. Microsoft made available a free patch for customers using versions of its Internet Information Server software with its Windows NT or Windows 2000 operating systems. The server software included within Microsoft's newer Windows XP operating system was not affected by the security flaw.

http://news.findlaw.com/ap/ht/1700/6-12-2002/20020612170005\_59.html

09

Category 23.6 Web-site infrastructure, general Web security issues

2002-06-18 quality assurance QA alert vulnerability snafu problem bug notification patch

FindLaw Download This 90

## SECURITY FLAW IN WEB SOFTWARE

A security bug was found in software used by millions of Web sites. Private experts alerted users and the FBI's computer security division. Problem is, they didn't tell the maker of the software. Then they issued the wrong prescription for fixing the problem. The incident Monday involving Apache's Web software shows that the system to insulate the Internet from attack - a joint effort of the government and private companies - is still a long way from perfect. http://news.findlaw.com/ap/ht/1700/6-18-2002/20020618023004\_3.html

Category 23.6 Web-site infrastructure, general Web security issues

2002-12-11 Web hijacking imposter counterfeit spoofing fraud theft consumer

NewsScan

#### IMPOSTOR EBAY SITE SET UP TO STEAL CREDIT INFO

A Web site called ebayupdates.com, having no relation to the eBay auction site, was created as part of a scam to obtain credit information fraudulently from eBay customers. The scam was discovered by the private Internet watchdog group SANS Institute Internet Storm Center, and was confirmed by an eBay executive who said: "Some members have reported attempts to gain access to their personal information through e-mail solicitations that are falsely made to appear as having come from eBay. These solicitations will often contain links to Web pages that will request that you sign in and submit information. eBay employees will never ask you for your password." (Reuters/San Jose Mercury News 11 Dec 2002)

# Operating systems, network operating systems, TCP/IP problems (alerts)

Category 24 Operating systems, network operating systems, TCP/IP problems (alerts)
2002-01-19 operating system push-pop stack buffer overflows design
RISKS 21 87

Earl Boebert wrote a succinct summary of how easy it would be to prevent buffer overflows if any of several possible well-known designs were used in today's operating systems:

>In my view, attempts to close the buffer overflow vulnerability through software or compiler tricks are doomed to one degree of failure or another because you're trying to program around a stupid processor design. Certain contemporary processors actually host a Pantheon of stupidities, consisting of a Greater Stupidity and two handmaiden Lesser Stupidities.

Greater Stupidity: Read access implying execute access. Any piece of data that the processor can be tricked into loading into the command register immediately becomes code. This is a stupidity of such breadth and depth that it comes with an event horizon.

Lesser Stupidity I: Segmented addressing that isn't. Let's say you have an addressing scheme consisting of segment number plus offset. This raises the question of what to do when, in executing code, block moves, etc., the offset gets counted up to maximum length plus one. Smart answer: take a fault. Dumb answer: set offset to zero and count up one in segment number.

Lesser Stupidity II: Brain-dead stack design. If you enumerate the design space of dynamic storage management, you may realize that one actually has to \*work\* to produce a stack design so dumb that overflow attacks are possible. Here are four classes of designs that are immune to the vulnerability:

- 1. Descriptor stacks. The only thing that goes in the stack are addresses, preferably with a bounds value attached. Overflow a buffer and at worst you clobber the heap. Penalty: one level of indirection, which (The Horror! The Horror!) may cause your dancing pigs to dance slower than the other guy's. Possibility: can be fitted transparently to existing processor designs, assuming anybody cared.
- 2. Stack per protection domain. This assumes you can find the perimeters of your protection domains. Also slows down dancing pig displays because of copying parameters from stack to stack.
- 3. Separate control and data stacks. CALL/RETURN works the control stack, PUSH/POP works the data stack. Doh.
- 4. Error-checking stacks. A whole raft of options, including "shadow stacks" with checksums, return addresses protected with trap bits, etc. etc.

So, if it's all so straightforward and well known, why hasn't some vendor or other fixed it? Answer: the dancing pigs have won.

# 24.1 Windows 9x/Me/XP

Category 24.1 Windows 9x/Me/XP

2002-08-07 proprietary code open source Windows antitrust settlement court order intellectual

property patents

NewsScan

## WINDOWS CODE RELEASED TO DEVELOPERS

Complying with provisions of the proposed antitrust settlement with the Justice Department, Microsoft has begun giving independent software developers technical information about the Windows operating system, which will be used to create alternative Web browsers and other software products to rival ones offered by Microsoft. But the company's critics remain unappeased and vocal. Mike Pettit of ProComp, a trade group backed by Microsoft's competitors, says he has found "several examples where if you unclick a choice indicating you don't want to use Microsoft middleware, it shows up anyway... I find astonishing at this stage of the game that these kinds of things would happen. Either the Justice Department didn't do a very good job of protecting consumers or Microsoft has not done a very good job of compliance." (Los Angeles Times 6 Aug 2002)

## 24.2 Windows NT/2K

Category 24.2 Windows NT/2K

2002-07-17 standards vulnerability assessment defaults parameters operating system

NewsScan

## SETTING STANDARDS TO PROTECT THE INTERNET

In support of the nation's homeland security, the nonprofit Center for Internet Security (CIS) has forged a technical consensus among a large group of government agencies and private businesses. The focus of the plan is largely on the widely used (though not the latest) Microsoft Windows 2000 operating system, and uses a software "scoring" system to ensure that specific technical security settings are properly in place. Government agencies participating in the security review included the Pentagon, NSA and NIST, and corporations included Allstate, First Union, Visa and Pacific Gas & Electric. (Washington Post 17 Jul 2002)

Category 24.2 Windows NT/2K

2002-10-21 spam penetration pop-up Windows operating systems warnings

NewsScan

## POP-UP SPAM -- A DIABOLICAL INVENTION

As if e-mail spam weren't annoying enough -- now there's pop-up spam. A Romanian-based company has developed software that can blast computers with pop-up messages through the Messenger function on many Windows operating systems that was originally designed to allow computer network technicians to warn network users of a planned shutdown (not to be confused with Instant Messenger). Gary Flynn, a security engineer at James Madison University, deplores this latest technological development: "It's almost like somebody barging into your office and interrupting you." Zoltan Kovacs, founder of the company that makes the software, responds, "If some people use it for bad things, they should take their own responsibility, but it's their own problem." The new spam technique represents the latest attempt by advertisers to bypass the increasingly sophisticated e-mail filters used by ISPs and individuals, and also circumvents state and other laws designed to curb junk e-mail. (AP 20 Oct 2002)

http://apnews.excite.com/article/20021020/D7MPIALG0.htm

## 24.3 UNIX flavors

Category 24.3

UNIX flavors

2002-01-20

vulnerability flaw quality assurance QA penetration weakness operating system OS UNIX TCP/IP malformed packet patches

Security Wire Digest

5

## CERT ISSUES NEW WARNING FOR OLD FLAW

Attackers are now actively exploiting a 2-month-old CDE vulnerability in Sun Microsystems' Solaris and other Unix OSes to break into servers on the Internet, say researchers at the Honeynet Project. According to published reports, researchers believe the vulnerability was first exploited in the wild last week. The buffer-overflow flaw, which affects Solaris, IBM's AIX, HP-UX and other Unix OSes, allows a specially crafted packet of Internet data to give an attacker full system access. Details of the vulnerability were published in a November CERT advisory. Security experts recommend administrators install corresponding patches, and limit or disable access to the vulnerable service.

http://www.cert.org/advisories/CA-2002-01.html http://www.cert.org/advisories/CA-2001-31.html

Category 24.3

UNIX flavors

2002-05-05

operating systems command interpreters standards assumptions differences dialects user interface UNIX LINUX GNU

RISKS

22

05ff

Theo Markettos provided an interesting warning about assuming anything about command structures in different dialects of UNIX:

\*\*\*

Under HPUX, killall kills \_every\_ process, except those required for shutdown. It takes an optional signal argument, but ignores this if it doesn't recognise it as a valid signal name. Hence 'killall httpd' kills everything except a handful of processes required for shutdown. If not running as root, it kills all processes owned by the current user.

The RISK? Don't assume something that is safe on one OS is on another, and don't assume that running a command without arguments to get help will do the right thing.

\*\*\*

Markettos' short comment provoked a flurry of rants and counter-rants in subsequent issues of RISKS; one quibble was that Linux is not UNIX (Richard Stallman once suggested it be spelled "LiGNUx"). Another comment I liked was that a well-designed command interpreter should question the presence of parameters following a command when it doesn't expect them, just as it would question the absence of required parameters.

Category 24.3

UNIX flavors

2002-08-16

open-source Linux Windows activists legislation government

#### NewsScan

#### OPEN-SOURCE ACTIVISTS SAY: GIVE US LIBERTY FROM MICROSOFT

A group of just 30 of the 15,000 Linux World conference attendees in San Francisco staged a rally outside City Hall to urge politicians to adopt the Digital Software Security Act, which would require California state agencies to use open-source software such as Linux as an alternative to Microsoft Windows. A leader of the group proclaimed, "Government and monopolists want to take away our right to write software and use computers as we want to use them. Open source is the true spirit of democracy, and we must preserve it." The Computing Technology Industry Association, a Washington, D.C.-based industry trade group, charged that the proposed Digital Software Security Act -- which is supported by an array of hackers, civil libertarians, and critics of Microsoft -- would stifle innovation in corporate America and have unintended adverse consequences. (AP/New York Times 15 Aug 2002)

Category 24.3 UNIX flavors

2002-09-16 LINUX operating system corporate applications acceptance

NewsScan

## LINUX IN THE CORPORATE WORLD

The Linux operating system, which has already found a secure place in academic and government computing environments, is becoming increasingly attractive to corporate information technology managers seeking less-costly alternatives to the offerings of Microsoft and Sun. IBM is now expanding its foray into the corporate Linux world, by announcing a multi-year alliance with Red Hat, the largest company in the marketplace that sells professional support for Linux, an "open-source" product available free (without support). Alliances such as these will ease the fears of corporate IT managers concerned about the compatibility issues of unsupported software. (New York Times 16 Sep 2002)

Category 24.3 UNIX flavors

2002-09-17 LINUX operating system applications acceptance office software universities digital divide international

#### NewsScan

#### SUN OFFERS SCHOOLS STAROFFICE SOFTWARE FOR FREE

Sun Microsystems took aim at Microsoft's dominant position as a supplier of office software for schools and is sponsoring a giveaway of its rival StarOffice product to ministries of education in Europe and South Africa. Sun hopes its donation, estimated to be worth \$650 million, will put StarOffice into schools serving some 26 million elementary, secondary and college students in those areas. The donation comes as something of a departure for Sun, which up until now has focused more on supplying relatively obscure software development tools to universities. The company's goal, says CEO Scott McNealy, is to destabilize Microsoft Office's dominance on the PC desktop and to erode billions of dollars of profit earned from sales of the software. The prevalence of Office in schools means that by the time children graduate, "they're going to be kind of hooked for life," says McNealy, who noted his initiative would also free up funding for other instructional expenses and student/teacher ratio reductions. (Wall Street Journal 17 Sep 2002)

Category 24.3 UNIX flavors

2002-09-18 LINUX operating system applications acceptance management

## NewsScan

## SUN TO PLAY LINUX CARD AGAINST MICROSOFT

Sun's strategy for competing against Microsoft has begun to revolve around the Linux operating system and the "open source" software movement, in which programmers around the world are given access to computer code and invited to suggest improvements. Sun executive Jonathan Schwartz thinks Microsoft is vulnerable because of the perceived security issues with some of its products and because Sun has a cost-advantage against Microsoft in providing service to corporate call centers that handle customer service, retail banking, and other such applications. Schwartz claims, "We can support 2,000 users with one system administrator at Sun. It requires in the neighborhood of one administrator for every 50 users in the Windows world." (New York Times 17 Sep 2002

## SUN'S LOW-PRICED LINUX SYSTEMS FOR CORPORATE USE

In its continuing battle against Microsoft for the PC desktop marketplace, Sun soon will be offering inexpensive Linux-based machines targeted for call centers other corporate environments that require a limited set of features. A statement from Sun says, "The primary motivator for enterprise customers will be reduction in costs and freedom from Microsoft." The systems (called the "Mad Hatter" at Sun) will cost about \$1,000, including monitor, and will be sold in lots of 100 along with a computer server and a services fee. (Reuters/San Jose Mercury News 18 Sep 2002)

Category 24.3 UNIX flavors

2002-11-18 Linux Windows personal computers PCs consumer sales

NewsScan

## WAL-MART SELLS WINDOW-LESS COMPUTERS

Wal-Mart's online shopping site has started selling inexpensive computers, priced in the \$299 to \$599 range, that feature the Linux-based LindowsOS operating system. Lindows' Web site says "LindowsOS computers come with software to view, print and copy MS Word files, MS PowerPoint files and MS Excel files," but they lack the software necessary to run those programs. Instead, the LindowsOS computers support alternatives such as the free OpenOffice software suite. Wal-Mart said its move comes in response to customers asking for machines loaded with Linux, but it has no plans to sell them in its stores. (AP 16 Jul 2002)

http://apnews.excite.com/article/20020716/D7KQADA80.htm

## LINUX, IN DAVID VS. GOLIATH BATTLES, CONTINUES TO MAKE HEADWAY

Little Linux, the home-grown, fast-growing, open-source operating system that invites code-enhancements from programmers all over the world, continues to make headway in the so-called real world: Wall Street, Hollywood, and government. Industry analyst Bill Claybrook of the Aberdeen Group says the operating systems wars will come down to two players, with Sun's Unix offering eventually falling in battle: "The real horse race, long-term, is going to be between Linux and Windows." [Yes, we've mixed some metaphors here. Be quiet.] Microsoft, unsurprisingly, thinks that victory is theirs, but Linux supporters believe that the bigger they are the harder they'll fall. Surprisingly, money may be the ultimate deciding factor, and one information services executive who just opted for Linux in his company explains: "We wanted to run it on Linux because it was quick and easy to launch. Plus, it was a fraction of the cost of a Microsoft license." (USA Today 5 Aug 2002)

#### SUN'S NEW LINUX STRAGEGY

Sun Microsystems is introducing its first line of computers using the Linux operating system, created and distributed as "open source code" by the Finnish programmer Linus Torvalds, and then further developed by volunteer programmers throughout the world. The pricing of Sun's LX50 server will begin at \$2,795, making it very competitive with Dell's system running the red Hat version of Linux and costing about \$3,700 for a similarly configured system. Sun seems to be shifting away from its "thin client" strategy, which uses inexpensive terminals that rely on powerful centralized computing, and instead embracing the Linux operating systems and its low-cost StarOffice software suite for word processing, spreadsheet, and other business applications. Sun is hoping to persuade large corporations to abandon Microsoft software applications: "Our target is the telephone-call center that wants to put software on 10,000 desktops," says Sun executive Jonathan Schwartz. (New York Times 12 Aug 2002)

#### THE LINUX ASSAULT ON MICROSOFT

Although Linux has proven quite successful in the server market, it has had trouble penetrating the desktop market because Microsoft's Windows software comes bundled with most new PCs. The new hope of Linux enthusiasts is that the release of LindowsOS 2.0 as a \$129 standalone product will create new momentum in the war against Microsoft domination. The new Lindows product will support dozens of Linux applications (including ones that mimic Windows applications), will include Sun's StarOffice 6.0 word processing software, and will support more than 800 printers. The software will also be available on an inexpensive tablet computer scheduled for release in early 2003. (ZDNet 18 Nov 2002)

Category 24.3 UNIX flavors

2002-12-19 Linux consumer electronics

NewsScan

## SONY, MATSUSHITA TO DEVELOP LINUX SYSTEM

Sony and Matsushita Electric are teaming up to develop an operating system based on Linux technology that will be incorporated into their digital consumer electronic products, such as televisions, DVDs and microwave ovens. The decision is likely to increase competitive pressure on Microsoft. Computer heavyweight IBM and several other high-tech companies have also embraced open-source software, particularly Linux, in their offerings. Matsushita and Sony say they are considering expanding the use of their jointly developed OS with other interested electronics companies, including Hitachi, IBM, NEC, Philips, Samsung and Sharp. The source code will also be made available free to the public to encourage its broader use throughout industry. (AP 18 Dec 2002)

http://apnews.excite.com/article/20021218/D7O09AEG2.htm

# 24.6 WAP, WEP, Wi-Fi, Bluetooth, 802.11

Category 24.6 WAP, WEP, Wi-Fi, Bluetooth, 802.11

2002-01-25 wireless tunneling firewall network workstation

RISKS 21 89

Jeremy Epstein noted in RISKS that, "Wireless carriers including Sprint, Cingular, and Seven (a startup) are putting together products that tunnel through the firewall to allow you to access the e-mail, calendars, etc. on your desktop machine remotely from a wireless device. . . . "

http://www.infoworld.com/articles/hn/xml/02/01/28/020128hnport.xml

Category 24.6 WAP, WEP, Wi-Fi, Bluetooth, 802.11

2002-01-28 wireless networks Wi-Fi vulnerability implementation installation problems

weakness ban

## NewsScan

## WIRELESS TECHNOLOGY CRITICIZED FOR VULNERABILITIES

Lawrence Livermore National Laboratory in California has banned all wireless networks, including Microsoft's Wi-Fi, because of security concerns. Wi-Fi supporters say the technology is secure when it's been properly installed, but experts say that only about 10% of all users install them correctly. (USA Today, 28 Jan 2002) http://www.usatoday.com/life/cyber/tech/2002/01/29/wifi.htm

Category 24.6 WAP, WEP, Wi-Fi, Bluetooth, 802.11

2002-02-20 wireless security Wi-Fi 802.1X protocol weakness man-in-the-middle attack hot spots session hijacking

spots session injacking

RISKS, http://www.pcworld.com/news/article/0,aid,84424,00.asp 21 92

Prof. William Arbaugh and graduate student Arunesh Mishra of the University of Maryland published a paper entitled, "An Initial Security Analysis of the IEEE 802.1X Standard" in which they demonstrated specific methods of session hijacking in the Wi-Fi protocol. Hijacking involves monitoring the authentication process and then sending a forged "disassociate" message apparently from the access point. The attacker then continues using the established session while the original user simply assumes there's been a communications error and establishes a new connection.

Category 24.6 WAP, WEP, Wi-Fi, Bluetooth, 802.11

2002-03-14 hacking tools cost ease wireless networks eavedropping

RISKS, http://news.bbc.co.uk/hi/english/sci/tech/newsid\_1860000/1860241.stm 21 96

Wireless networks can be hacked easily, in part using directional antennas made from discarded Pringles potato-chip tubes.

Category 24.6 WAP, WEP, Wi-Fi, Bluetooth, 802.11

2002-04-01 satellite radio wireless communications interference jamming Wi-Fi frequencies

NewsScan

## SATELLITE RADIO OPERATORS COMPLAIN ABOUT WI-FI INTERFERENCE

XM Satellite Radio and Sirius Satellite Radio have petitioned the FCC to regulate Wi-Fi technology more closely, threatening to stymie innovation in the nascent wireless technology market. The satellite radio broadcasters say that even though Wi-Fi operates on a different frequency, the frequencies are so close that it's possible for energy to leak over from Wi-Fi devices and interfere with their services. They're asking the FCC to set limits on the services, although they say they're not trying to shut them down. "I think wireless devices are going to blossom," says Sirius co-founder Robert Briskman, who says Wi-Fi device manufacturers could alleviate the problem by installing filters and making other changes to wireless transmitters. Wi-Fi advocates say their systems comply with current FCC rules and that if the satellite radio folks are worried about interference, they should tinker with their own systems. Meanwhile, FCC Chairman Michael Powell is keeping mum on the satellite proposals, but has cautioned that heavy usage of Wi-Fi and other devices that use unlicensed frequencies could eventually cause a "meltdown." (Wall Street Journal 1 Apr 2002)

http://online.wsj.com/article/0,,SB1017613134883515920.djm,00.html (sub req'd)

## XM, DELPHI TEAM UP ON PORTABLE SATELLITE RADIO DEVICE

XM Satellite Radio and auto parts maker Delphi unveiled their Delphi XM SKYFi Radio receiver -- a pocket-sized portable device that enables listeners to tune into XM's satellite radio channels using a home stereo system or a portable boombox. The device, which will be available in stores next month, will be priced around \$130. The kit to connect it to a home or car stereo will retail for around \$70. XM says it's received orders from retailers for between 120,000 and 150,000 units and expecting brisk sales through the holiday season. The company is hoping to have 350,000 subscribers by the end of the year. (Reuters 25 Sep 2002)

http://makeashorterlink.com/?H27252BE1

Category 24.6 WAP, WEP, Wi-Fi, Bluetooth, 802.11

2002-04-11 Radio Frequency Identification Tags REIG Electronic Product Code ePC privacy

wireless communication

NewsScan

## THINGS COME ALIVE

We're just at the beginning of a new age of products, devices and objects that talk to us -- and to each other. "We're really talking about the next 50 years of computing," says the executive director of the Auto-ID Center at MIT, which is one of the organization studying ways of using computer chips embedded in tiny pieces of plastic attached to just about everything, including egg cartons, eyeglasses, books, toys, trucks, and money. The tags are currently known as Radio Frequency Identification Tags (REIG), and the Auto-ID Center calls the core of its standard "ePC" or Electronic Product Code. Companies such as Wal-Mart, Gillette, and Procter & Gamble have committed to using the technology. As for privacy issues? Accenture scientist Glover Ferguson agrees that privacy will be an issue, and says: "There will have to be a social discourse about what we want and don't want. But the technology isn't going away. You can't un-invent it." (USA Today 11 Apr 2002) http://www.usatoday.com/life/cyber/tech/2002/04/12/tinyband.htm

Category 24.6 WAP, WEP, Wi-Fi, Bluetooth, 802.11

2002-05-23 wireless cash registers hackers theft fraud penetration eavedropping

RISKS; http://www.msnbc.com/news/746380.asp

22

According to a report by Bob Sullivan of MSNBC, several large retail stores, including Best Buy, Walmart and Home Depot are using unencrypted traffic over wireless point-of-sale devices. Experimenters (perhaps more usually known as "hackers") monitoring traffic from parking lots at the stores claimed to have picked up sensitive data such as customer credit-card numbers in transit.

Category 24.6 WAP, WEP, Wi-Fi, Bluetooth, 802.11

2002-06-12 Wi-Fi wireless ISP Internet service provider

NewsScan

## EARTHLINK TO OFFER WI-FI SERVICE

EarthLink is marketing its "EarthLink Wireless High Speed" service to customers eager to take advantage of about 650 Wi-Fi networks in coffee shops, hotels, airports and other public spaces throughout the country. The deal makes EarthLink among the first traditional ISPs to sell services based on the Wi-Fi wireless networking standard. Analysts say many ISPs are interested in selling Wi-Fi services, but have been waiting on the sidelines for heavyweights, like EarthLink or AOL, to make the first move. "This is what people have been waiting for: stronger backing by service providers," says an analyst with Synergy Research Group. EarthLink's service is offered in conjunction with Wi-Fi networking firm Boingo Wireless, a startup headed by EarthLink founder Sky Dayton. EarthLink customers will use Boingo's networks, and have the option of buying access in 24-hour chunks, during which they can log on and off as many times as they choose. A single "day pass" costs \$8, or customers may purchase a package of 10 "day connects" for \$25. (CNet News.com 11 Jun 2002) http://news.com.com/2100-1033-935034.html?tag=fd\_top

Category 24.6 WAP, WEP, Wi-Fi, Bluetooth, 802.11

2002-07-25 broadband services sharing piracy contract wireless

NewsScan

## BROADBAND PROVIDERS CRACK DOWN ON 'SHARING'

Broadband providers are not looking kindly on some subscribers' hobby of "sharing" their high-speed connections with friends and neighbors who pay nothing. Time Warner Cable recently sent letters to 10 subscribers in New York giving them three days to cease their sharing activities, and threatening to cut off their service if they failed to do so. "When you contract for high-speed access, it's for your use in your household and not to share with neighbors," says a Time Warner spokeswoman. Meanwhile, AT&T Broadband also plans to contact connection-sharing users. In both cases, subscribers need simply to install an antenna on the roof of their house, which enables up to 50 people to use the connection. The signal can travel as far as 20 miles. (Investor's Business Daily 25 Jul 2002 -- print only)

Category 24.6 WAP, WEP, Wi-Fi, Bluetooth, 802.11

2002-08-12 wireless Wi-Fi standard telecommunications Internet access

NewsScan

## IS WI-FI THE FUTURE OF TELECOM?

Working with Athens, Georgia, to develop a wireless communications "cloud" over the city's downtown, Scott Shamp, the director of the University of Georgia's New Media Institute, says: "We're designing a sandbox. We want a place where people can experiment... This feels like the Internet from 1994." Will Wireless Fidelity (or WiFi) networks, based on the technical standard 802.11b, provide competition for the large telecom companies? Not just yet, but experts such as MIT Media Laboratory director Nicholas Negroponte recently told a Congressional committee that the telecom industry may not recover its former market value, because in the future "we're going to use telecommunications very differently." Wireless clouds can support a new generation of technology, including always-on portable digital devices and environmental sensors. The hope of WiFi enthusiasts is that the low-cost, grass-roots technology will grow "organically" into a nationwide communications system. (AP/San Jose Mercury News 12 Aug 2002)

Category 24.6 WAP, WEP, Wi-Fi, Bluetooth, 802.11

2002-09-11 Wi-Fi roaming sharing network ISP Internet service provider penetration wireless communications e-commerce billing payment

NewsScan

## WI-FI FANS WANT TO ROAM

The popularity of Wi-Fi -- the wireless networking technology that broadcasts an Internet connection over a radius of 300 feet -- is spawning efforts to expand the service so that customers of one wireless provider could use the network of another. The barrier lies not in the technology, but in the billing technicalities. "The bits, the bytes and the hardware exist for roaming. We just need someone to start pulling it all together," says Barry Davis, Intel's director of platform architecture. And while a technical standard isn't required to create roaming capability, there is industry pressure on the IEEE (Institute of Electrical and Electronic Engineers) and the ETSI (European Telephone Standards Institute) to agree one, because it would cut costs and help jumpstart the development of future Wi-Fi technology. Meanwhile, some Wi-Fi carriers are teaming up on their own: Boingo Wireless, the second-largest U.S. carrier, has already established roaming agreements with two other wireless providers and is looking for more. In Europe, a number of companies, including Swiss carrier Monzune, are testing Wi-Fi roaming, and in Japan, Multimedia Mobile Access Communication Systems has created its own wireless roaming standard. "The Asian market is getting faster adoption, and the Europeans are next in line," says John Baker, CEO of Transat, which makes software that enables Wi-Fi roaming. (CNet News.com 10 Sep 2002) http://news.com.com/2102-1033-957411.html

Category 24.6 WAP, WEP, Wi-Fi, Bluetooth, 802.11

2002-09-30 wardriving wireless law enforcement scanning security vulnerabilities commercial

networks

NewsScan

## WIRELESS 'WARDRIVING'

Secret Service agents in Washington are driving the city's streets (in an effort called "wardriving") to detect security holes in wireless communications systems. Special Agent Wayne Peterson says, "Everybody wants wireless, it's real convenient. Security has always been an afterthought." He regards what he is doing as a normal part of police work, and compares it to a patrolman driving through a neighborhood to make sure everyone is safe. When he or his colleagues find a security gap, they report it to the companies that operate the vulnerable wireless networks, so that the problem can be fixed. The Secret Service calls security holes in wireless communications systems one of the most overlooked threats to computer networks. (AP/San Jose Mercury News 30 Sep 2002)

Category 24.6 WAP, WEP, Wi-Fi, Bluetooth, 802.11 2002-10-30 wireless ISP Internet service provider

NewsScan

#### WIRELESS BROADBAND MAKES SPLASH

A new wireless Internet service provider is offering its customers speeds up to 20 times faster than typical dialup services using the CDMA20001xEV-DO standard. By November, Monet Mobile Networks plans to offer its Monet Broadband service in cities in North Dakota, South Dakota and Wisconsin. EV-DO, as it's nicknamed, offers downloads at speeds up to 2.4Mbps, and leading wireless carriers Verizon Wireless and Sprint PCS may be considering building EV-DO networks by 2005. Both companies now use the CDMA standard, which is adaptable to the faster version. Verizon says it is already testing EV-DO networks in San Diego and Washington, DC. Meanwhile, Monet plans to focus its business strategy on bringing broadband Internet access to rural areas, which typically are underserved. "We've received tremendous welcome by these communities which have been overlooked by most of the technology sector," says a Monet spokesman. For \$40 a month, Monet subscribers get unlimited Web access, three e-mail addresses and 5MB of data storage. An alternative plan offers five accounts and 25MB of storage for \$60 a month. (CNet News.com 29 Oct 2002)

http://news.com.com/2100-1033-963808.html?tag=fd\_top

WAP, WEP, Wi-Fi, Bluetooth, 802.11 Category 24.6

2002-11-13 wireless tokens I&A identification authentication tracing monitoring surveillance

radio

NewsScan

## THE FUTURE OF COMPUTING WILL BE INVISIBLE

Computing power will be easier to harness as it pervades every corner of our lives, and at the same time will be increasingly transparent, according to an annual technology forecast from PriceWaterhouseCoopers. The proliferation of printable, lowpower, short-range radio ID tags will imbue many formerly dumb household appliances with "smart" computing power. Alongside these developments will go efforts to hide the difficulties of tying these devices together and managing large numbers of networked computers, phones or gadgets. "Users do not want to see that complexity," says PWC analyst Kevin Findlay. Meanwhile, businesses will discover the power of in-house grid computing, which from time to time could give a pharmaceutical firm, for instance, the processing power of a supercomputer, just by linking their own idle desktop machines. Findlay also noted that companies likely will move toward renting data storage as they need it, rather than buying it and having it sit idle. (BBC News 13 Nov 2002)

http://news.bbc.co.uk/1/hi/technology/2449009.stm

Category 24.6 WAP, WEP, Wi-Fi, Bluetooth, 802.11

2002-11-18 Wi-Fi wireless communications ISP Internet service provider

NewsScan

#### IS WIRELESS THE NEXT GREAT THING?

Life goes on even in a downturn, and there's always the next great thing around the corner. Many people now thing that next great thing will be Wi-Fi, the wireless Internet-access technology that allows anyone with an enabled computing device to connect to the Internet at high speeds and offers "location aware" communications capable of such tricks as showing you where the closest restaurant or movie theater is. The impact of wireless communications will be huge, both on business and on the way we live. Leslie L. Vadaz of the Intel Capital investment unit says, "There is no question in my mind that wireless 'bitways' will make the traditional communications business obsolete." And Ken Biba of the wireless communications company Vivato adds: "This feels like the opening of the PC era when for the first time you could own your own computer. With Wi-Fi you can own your own communications. That's a profound social change." (New York Times 18 Nov 2002)

Category 24.6 WAP, WEP, Wi-Fi, Bluetooth, 802.11

2002-11-22 Wi-Fi wireless ISP Internet service providers growth

NewsScan

## WI-FI REACHING MAINSTREAM

Verizon's announcement yesterday that it will install Wi-Fi wireless Internet technology for small and medium-size businesses is the latest sign that Wi-Fi is becoming a mainstream communications technology. Recently, T-Mobile and Boingo Wireless made similar moves, though Yankee Group analyst Sarah Kim characterized Verizon's position as "arguably in the forefront." Still, the big phone companies in countries such as South Korea, the United Kingdom, Sweden and Japan have been quicker to embrace Wi-Fi and install it to create wireless "hotspots" in public locations such as stores, cafes, airports and hotels. (AP/USA Today 22 Nov 2002)

http://www.usatoday.com/tech/news/digest.htm

Category 24.6 WAP, WEP, Wi-Fi, Bluetooth, 802.11

2002-12-05 wireless networks Internet access growth Wi-Fi

NewsScan

#### WI-FI: BIGGER THAN BUDWEISER?

To illustrate his vision of the future of Wi-Fi wireless networking, Wi-Fi Alliance chairman Dennis Eaton told attendees at the 802.11 Planet Conference that "We're looking at Budweiser potential, going forward." Citing revenue expectations of about \$2 billion this year, Eaton estimated that profits related to the wireless networking industry will grow at a compounded rate of 30% through 2006, surpassing revenue estimates of household products such as Budweiser beer, which will bring in about \$5 billion this year. Eaton says Wi-Fi's ability to complement other emerging technologies, such as broadband and next-generation cellular networks, will boost its growth, but the major obstacles in the industry remain consumer education about what wireless networking can do, what sort of transfer rates and range can be expected, and which standards are compatible. (CNet News.com 4 Dec 2002)

http://news.com.com/2100-1033-976076.html?tag=fd\_top

# 24.7 SWDR (Software-defined radio)

Category 24.7 SWDR (Software-defined radio)

2002-11-11 software defined radio SDR frequency spectrum overload

NewsScan

## SDR CAN SOLVE WIRELESS GADGET OVERLOAD

Software defined radio (SDR) technology may hold the key to developing a single standard for the numerous portable devices now on the market, thereby unlocking new opportunities for wireless communications. As the line between "smart" phones and PDAs blurs, the multifunctional devices are becoming cluttered with software designed for each specific activity. "You could have your cell phone going, be using a Bluetooth headset and at the same time use GPS to check where you are," says Mark Cummings, an SDR proponent who notes that without SDR, that scenario would require cramming three separate radio circuits into a single handset. John Watson, VP of marketing for QuickSilver Technology, says SDR software would enable handset design that's more flexible and able to respond to changing market demands. "Right now, you have to do electronics design a couple of years ahead of time" before bringing new equipment to market. "The only thing you know is you're going to be wrong. What you really want is to be able to design it at the last minute." (Wired.com 11 Nov 2002)

# 24.8 MAC OS

Category 24.8 MAC OS
2002-05-18 spam filtering documentation ISP Internet service provider
RISKS 22 07

A mild ruckus broke out when Mac OS users discovered undocumented spam filters on the free POP3/IMAP e-mail servers available to them through thye Apple company. Apparently the false positives were bouncing legitimate messages, but since the victims neither knew about the filtering nor (naturally) had any control over this function, there was very little they could do about it other than stop using the service.

# 24.9 Peer-to-peer networking

Category 24.9 Peer-to-peer networking

2002-01-07 privacy peer-to-peer spyware music swapping tracking Trojan game online

gambling quality assurance QUALITY ASSURANCE

NewsScan

## USER WEB HABITS TRACKED BY SOME MUSIC-SWAPPING PROGRAMS

The Web surfing habits of people who used the LimeWire, Grokster and KaZaA music-sharing programs were surreptitiously tracked because those programs were linked to an online sweepstakes game called ClickTillUWin, in which players pick numbers and win cash prizes. The company that operates the sweepstakes game says it told outside distributors to get users' permission before installing the software, but in these cases that action was not taken. The three companies have posted new versions of their software without the tracking component, and LimeWire has issued an apology. (AP/USA Today 4 Jan 2002) http://www.usatoday.com/life/cyber/tech/2002/01/04/limewire-tracking.htm

Category 24.9 Peer-to-peer networking

2002-01-24 unauthorized use prosecution plea-bargain fine probation encryption brute-force

distributed computing college

Security Wire Digest 4 6

## SYSADMIN GETS FINE, PROBATION FOR DISTRIBUTED COMPUTING

A computer technician who installed software for a volunteer distributed-computing effort was given probation and a \$2,100 fine this week after an agreement was reached with state prosecutors. David McOwen, who worked at DeKalb Technical College in Georgia, was officially charged with one count of computer theft and seven counts of computer trespassing. He could have faced years in prison and hefty fines and restitution for using DeKalb computers to assist in a communal codebreaking challenge, according to published reports.

Category 24.9 Peer-to-peer networking

2002-03-25 distributed computing scientific research search engine

NewsScan

## GOOGLE TACKLES DISTRIBUTED COMPUTING

Google has invited 500 users to try out a new version of its toolbar that enables them to donate their excess processing power to a Stanford University research project aimed at discovering how genetic information is converted into proteins. The Google Compute project follows the lead of other distributed computing endeavors that have sought to find everything from extraterrestrial life to cures for cancer and anthrax. "The main motivations were to try to leverage Google's expertise with large computer systems and to try to give something back to science," says Susan Wojcicki, head of Google Compute. The company likely will expand the program to include other scientific projects in an effort to boost its search business, says Wojcicki, but she doubts it will ever become a source of revenue in itself. "You never want to say never, but the goal now is to contribute something to science. We have enough fish to fry in our current businesses." (CNet News.com 22 Mar 2002) http://news.com.com/2100-1001-867091.html

Category 24.9 Peer-to-peer networking

2002-04-30 P2P peer-to-peer networks intellectual property file-swapping piracy copyright

violations

NewsScan

## PEER-TO-PEER SITES MULTIPLY DESPITE LEGAL PROBLEMS

The number of peer-to-peer Web sites has increased more than five-fold in the past year, according to a study by Websense, despite heightened efforts by record companies, movie studios and software makers to shut them down. According to the survey, the number of file-swapping sites totals nearly 38,000, up 535% in the last year. Meanwhile, the recent surge in file-swapping is beginning to affect the workplace, as employers struggle to deal with the issues surrounding workers who use the speedy corporate networks to download songs and software — a potentially illegal activity. "Companies that look the other way many have copyright violations occurring in the workplace, and lawsuits are a potential outcome of such activity," says one attorney. (Reuters/CNN.com 29 Apr 2002)

http://www.cnn.com/2002/TECH/internet/04/29/file.swapping.reut/index.html

Category 24.9 Peer-to-peer networking

2002-06-10 P2P peer-to-peer networks file sharing vulnerabilities privacy penetration hard drive

e-mail financial information compromise honeypot

RISKS 22 12

Nathan Good of the Information Dynamics Lab at HP Laboratories posted a note in RISKS:

We have just finished a study that shows how user interface design flaws allow users on Kazaa to share their personal files without their knowledge. In a laboratory user study, only 2 out of 12 subjects were able to correctly determine that Kazaa was sharing their entire hard drive. We looked at the current Kazaa network and discovered that many users are sharing personal information such as email and data for financial programs such as Microsoft Money.

To see if other users on Kazaa were aware of this and taking advantage of users ignorance, we ran a Kazaa client for 24 hours with dummy personal files. During this time, files named "Inbox.dbx" and "Credit Cards.xls" where downloaded from our client by several unique users.

The tech report can be accessed here: http://www.hpl.hp.com/shl/papers/kazaa/KazaaUsability.pdf or from our lab web page at http://www.hpl.hp.com/shl/

Category 24.9 Peer-to-peer networking

2002-09-13 wireless cellular mobile phone peer-to-peer P2P networking picture music

#### NewsScan

## TECHNOLOGY TURNS WIRELESS NETWORK INTO P2P PLAYGROUND

Apeera, based in France, has developed a technology that enables mobile phone users to set up an unlimited digital storage "cabinet" for their own media files and allows them to share the files with other cell phone users. Apeera's creators say the system could prove popular with wireless carriers eager to convert customers into multimedia services subscribers. "Peer-topeer is the cornerstone of making a service successful," says an Apeera spokesman. "Logos and icons are going to become pictures, ringtones are going to become music files." Apeera users can send files to any WAP- or Java-enabled phone, even if the recipient isn't signed up for the Apeera service. (BBC News 12 Sep 2002) http://news.bbc.co.uk/1/hi/technology/2253185.stm

# 24.A Secure processors

Category 24.A Secure processors

2002-06-25 operating system security monitor kernel hardware

NewsScan; http://apnews.excite.com/article/20020625/D7KC66M01.html

## MICROSOFT CREATES VIRTUAL 'VAULT'

Microsoft, bowing to pressure to make its Windows operating software more secure, is developing a new security feature called "Palladium" that acts as a virtual "vault" for conducting electronic transactions and storing sensitive information. In order to use the new feature, consumers will have to buy new computers equipped with ultra-secure computer chips from Intel, Advanced Micro Devices, among others. Microsoft says the new technology won't be available for at least 18 months, and company officials have said they don't expect to see Palladium-enabled products hit the mainstream market for at least five years. Supporters of the technology say it will be capable of weeding out viruses and other malicious computer code and that personal information such as financial or medical records will be encrypted and inaccessible, even from other software running on the computer. Critics say Palladium could end up being just one more means for Microsoft to dominate the world's software markets, and that using the software will require changes to video and keyboard technologies requiring billions of dollars in new equipment upgrades by consumers, corporations and governments. (AP 25 Jun 2002)

Category 24.A Secure processors

2002-09-10 secure microprocessor chips partitions operating systems

NewsScan

#### INTEL'S 'LEGRANDE' VISION FOR SECURE CHIPS

Intel is planning to build security features into its microprocessors next year, in a move aimed at thwarting computer viruses and malicious hackers. The technology, dubbed LeGrande, initially will be included in Prescott, the code name for a new Pentium chip due out the second half of 2003. The idea of using secure chips, in addition to software, isn't new, but gained wider attention this summer when Microsoft announced its Palladium security initiative, which it hopes to develop in conjunction with Intel and chip rival Advanced Micro Devices. Unlike Palladium, however, the LeGrande technology will work with operating systems other than Microsoft Windows. The technology works by partitioning off areas of the computer's hard drive into protected areas called "vaults," and protecting the pathways between the vaults and keyboards, monitors and other peripherals. (Wall Street Journal 10 Sep 2002)

Category 24.A Secure processors

2002-11-04 trusted computing hardware chips processors

NewsScan

## IT'S YOUR DATA; WHOM DO YOU TRUST WITH IT?

The major information technology companies, including Microsoft, Intel, IBM, Hewlett-Packard and 170 others, are developing an approach to data security called "trusted computing," which hardwires security into silicon chips and related software, rather than relying strictly on software to achieve security. Intel software manager Narendar Sahgal says, "This is a fundamentally new approach as opposed to taking a software-only approach." (At Intel trusted computing is called LaGrande; at Microsoft it's called Palladium.) In the trusted computing approach, each communication transaction (such as an e-mail message or an online purchase) is required to interact with secure and uniquely identified hardware through "trusted agents." Not all technologists are happy with the trend. Cambridge University security researcher Ross Anderson says, "I don't think the kind of trustworthiness they seek to deliver is at all desirable. It's not security for me. It's security for them." (AP/San Jose Mercury News 3 Nov 2002)

# 25.1 Remote control, RATs, reprogramming, auto-updates

Category 25.1 Remote control, RATs, reprogramming, auto-updates

2002-01-08 remote control FPGA field-programmable logic array firmware

RISKS 21 87

J. P. Gilliver noted an alarming development in remote reprogramming -- an easy way to modify firmware: "... For example, IRL (Internet Reconfigurable Logic) means that a new design can be sent to an FPGA in any system based on its IP address." (From Robert Green, Strategic Solutions Marketing with Xilinx Ltd., in "Electronic Product Design" December 2001. Xilinx is a big manufacturer of FPGAs.) For those unfamiliar with the term, FPGA stands for field-programmable logic array: many modern designs are built using these devices, which replace tens or hundreds of thousands of gates of hard-wired logic.

The RISKs involved are left as an exercise to the readers."

Category 25.1 Remote control, RATs, reprogramming, auto-updates

2002-01-16 theft deterrent remote control explosion destruction tampering interception data

diddling man-in-the-middle attacks criminal hackers vulnerability potential

## NewsScan

#### EXPLODING CHIPS COULD FOIL THIEVES

Researchers at the University of California in San Diego have developed a way to blow up silicon chips using an electric signal — an innovation that could be used to fry electronic circuitry in devices after they're stolen or fall into the wrong hands. The American spy plane that was impounded in China last year is an example where such technology would have proven handy in destroying its secret electronics systems. Similarly, if a cell phone were stolen, the owner could alert the wireless carrier, which would send a signal to trigger a small explosion in the phone's chip, rendering it useless. The techniques uses a small amount of the oxidizing chemical gadolinium nitrate applied to a porous silicon wafer. (New Scientist 16 Jan 2002) http://www.newscientist.com/news/news.jsp?id=ns99991795

Category 25.1 Remote control, RATs, reprogramming, auto-updates

2002-01-25 remote control firmware reprogramming update configuration change SMS

RISKS 21 89

In Switzerland, the mobile phone company Swisscom admitted that it reconfigured its customers' phones using a program embedded in a SMS (short message service) transmission. The message deleted roaming information. S. Llabres reported in RISKS, "... [I]nsiders believe that the modification of the roaming information was to direct traffic to networks owned by Vodafone -- which acquired a 25% share of Swisscom [in April] last year." Llabres commented astutely, "It would be interesting:

- \* If there is any security mechanism protecting anyone from sending such "special" messages.
- \* Which setting[s] on the mobile phone can be changed (or probably retrieved from the phone) without knowledge to the customer.
- \* If the network provider must implement such features, I do not understand why this must happen unperceived by the customer. Why not send a message telling people what will happen?"

Category 25.1 Remote control, RATs, reprogramming, auto-updates

2002-02-15 remote control self-updating programs essay article summary

RISKS 21 92

Scott Schram "published an article addressing some risks of programs that update themselves. Rather than a bona-fide update, the auto-update feature could be used to send programs with undesired features. The activity of these updaters would not be detected by firewall tools, as they are expected to be periodically checking for updates and downloading them. Further, the most careful reverse-engineering of the updater would not reveal anything unexpected."

http://schram.net/articles/updaterisk.html

Category 25.1 Remote control, RATs, reprogramming, auto-updates

2002-02-20 auto-update firewall Trojan trust

RISKS 21 92

Scott Schram published a paper at < http://schram.net/articles/updaterisk.html > that pointed out the security risks of all auto-update programs (e.g., self-updating antivirus products, MS Internet Explorer, MS-Windows Update, and so on). Once the firewall has been set to trust their activity, there is absolutely no further control possible over what these programs do. If any of them should ever be compromised, the results on trusting systems would be potentially catastrophic.

Category 25.1 Remote control, RATs, reprogramming, auto-updates

2002-03-14 automated aircraft collision detection avoidance robots

RISKS 21 96

In March 2002, tests on unmanned remote-control aircraft studied the effectiveness of automated collision-avoidance systems. Look for exciting developments in security-engineering failures in years to come.

Category 25.1 Remote control, RATs, reprogramming, auto-updates

2002-03-18 automated automobile highway monitoring detection surveillance

RISKS 22

In Boston, city engineers described plans for a new highway-traffic monitoring system called the Integrated Project Control System (IPCS). Using magnetic loops embedded in the pavement, the system would sense traffic speed and instantly report sudden slowdowns or stoppages as well as simply keeping track of total volume and speed for statistical purposes.

Category 25.1 Remote control, RATs, reprogramming, auto-updates

2002-04-22 critical infrastructure security wireless interception hijacking vulnerabilities

RISKS 22 04

John McPherson noted in RISKS:

http://www.nzherald.co.nz/storydisplay.cfm?storyID=1392336&thesection=technology&thesubsection=general

He added: "Now I don't know if this technology is mature enough to be trusted for this type of thing - I guess I'll wait for the comments to come flooding in. I sincerely hope they've thought through the encryption and security issues here."

Category 25.1 Remote control, RATs, reprogramming, auto-updates

2002-04-26 anti-collision technology automobiles crash lidar smart roadways

NewsScan

## 'SMART CAR' FEATURES BEGINNING TO SHOW UP IN LUXURY CARS

The widespread use of "adaptive cruise technologies" to prevent automobile collisions is still well in the future, but some luxury cars such as Infinti, Lexus, and Mercedes-Benz are now being offered with expensive options designed to allow moving vehicles to communicate with each and to detect sensors embedded in the pavement that detect the vehicle ahead either by radar or lidar (the laser-based equivalent of radar). Steven Schladover of the California Partners for Advanced Transit and Highways says: "It feels like you're in a train -- a train of cars. You don't see any separation between the vehicles, and, after a minute of feeling strange, most people relax and say, 'Oh, this is pretty nice!" A lidar package for the Infiniti Q45 will require purchase of a \$10,000 optional equipment package. (San Jose Mercury News 26 Apr 2002) http://www.siliconvalley.com/mld/siliconvalley/3143626.htm

<sup>&</sup>quot;... The Matamata wireless link replaced an expensive frame relay service as well as providing a 1Mbs Internet service to several outlying sites including a library and remote management of water supplies. As the water facilities are computer controlled, they are able to manipulate them remotely rather than sending someone 20 miles down the road just to turn a valve." ... From \*The New Zealand Herald\* (Talking about 802.11b)

Category 25.1 Remote control, RATs, reprogramming, auto-updates

2002-06-21 credit card keystroke capture Trojan Horse investigation law enforcement evidence

forensics university

Edupage; http://chronicle.com/free/2002/06/2002062001t.htm

## ASU PCS SEIZED IN INVESTIGATION

State police have confiscated desktop computers and hard drives at Arizona State University on the suspicion that unknown third parties installed keystroke-capture software on the computers with the goal of recording credit-card numbers and other personal data. Most of the affected systems were in open-use kiosks, according to campus representatives. The U.S. Secret Service is leading the investigation, with help from Arizona State Police. Computer systems at other colleges may also be involved. Speculation targets the Russian mafia as the perpetrators. Chronicle of Higher Education, 20 June 2002

## 25.3 RFI, HERF, EMP/T

Category 25.3 RFI, HERF, EMP/T

2002-07-24 spectrum wireless shortage dearth competition overlap

NewsScan

## FCC STEPS UP SEARCH FOR MORE SPECTRUM

A shortage of airwaves is hampering the U.S. wireless industry, and analysts say a major spectrum expansion is critical if the industry is to avert an erosion in the quality of cell phone service or a financial meltdown in the next two years. Although wireless companies are spending nearly \$10 billion this year to expand calling capacity and provide new high-speed data services, revenue per minute has dropped to 14 cents, down from 52 cents in 1992. "There's a basic rule of economics: If you sell something for \$1 that costs you \$1.05, you can't make money," says one telecom consultant. In an effort to alleviate the problem, the FCC announced last week it would auction 740 wireless licenses beginning next month, but those licenses are for spectrum now in use by television broadcasters, and some wireless operators have opposed the auction because carriers would be forced to spend hundreds of millions of dollars on spectrum that's not immediately available. "The wireless revolution is becoming a victim of its own success," says FCC wireless bureau chief Thomas Sugrue. "The simple truth is that as our society grows increasingly dependent on wireless technology and services, spectrum demand is stressing that supply, and that has made spectrum management difficult for government." (Los Angeles Times 5 Jul 2002) http://www.latimes.com/technology/la-fi-wireless5jul05

#### PLAN SHIFTS SPECTRUM FROM GOVERNMENT TO WIRELESS USE

The National Telecommunications and Information Administration has unveiled a plan to shift 90 megahertz of spectrum from government to commercial use in an effort to provide the additional airwaves the wireless industry says it needs for so-called third-generation (3G) wireless services. At least half the spectrum will come from the military, with the remainder coming from airwaves controlled by the Federal Communications Commission. Congress is expected to introduce legislation that would transfer the revenue from the auctioned spectrum to the military to cover the costs of buying new equipment and transitioning to different airwaves. Wireless companies could bid on the new spectrum as early as 2004, but wouldn't be able to use it until 2008, which is the earliest the military was willing to make the move. Analysts cautioned that the proposal is not entirely good news for the wireless industry, which has long complained it needs more spectrum to deliver advanced services. The 90 megahertz is less than half the 200 megahertz sought by the industry, and the two chunks are not contiguous, which will make it more expensive to use them. There's also the risk that the military might renege on the agreement down the road, arguing it needs the spectrum for national security requirements. (Wall Street Journal 24 Jul 2002)

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

Category 26 Health effects of electronic equipment (phones, screens, etc.)

2002-02-20 RFI radio frequency interference emissions wireless communications health danger

fraud lawsuit regulation

#### NewsScan

#### FTC SUES SELLERS OF CELL PHONE "RADIO SHIELD" [20 Feb 2002]

The Federal Trade Commission is suing two companies for selling devices purporting, without good evidence, to shield people from harmful radiation emitted by their cell phones. The small metallic devices were sold under such names as WaveShield 1000, NoDanger, and SafeTShield. The FTC said that by claiming that their products could "block up to 97% to 99%" of electromagnetic radiation," the companies were actually "using a shield of misrepresentation to block consumers from the facts." Among the facts missing in company sales materials is any mention of a 2001 General Accounting Office report indicating that "scientific research to date does not demonstrate that the radio frequency energy emitted from mobile phones has adverse health effects, but the findings of some studies have raised questions indicating the need for further investigation." (Newsbytes/Washington Post 20 Feb 2002)

http://www.washtech.com/news/telecom/15264-1.html

Category 26 Health effects of electronic equipment (phones, screens, etc.)

2002-04-18 toxic matrials hazardous waste disposal recycling

#### NewsScan

## LANDFILLS REJECT COMPUTER JUNK

What to do with old computers? Most landfills are refusing to accept them, because computer monitors and TV screens contain lead, mercury, cadmium and other hazardous materials that seep into soil and groundwater when they're crushed or burned. Well, can you give them to charitable organizations? Maybe, maybe not. Many refuse to accept them, because they can't afford to pay the disposal fees. One solution would be to use "pay-as-you-throw" programs offered by companies such as Hewlett-Packard and IBM, which charge \$13 to \$34 to pick up old computers. (San Jose Mercury News 17 Apr 2002) http://www.siliconvalley.com/mld/siliconvalley/3085767.htm

## 26.1 Radiation

Category 26.1 Radiation

2002-05-24 wireless cellular phone radiation standards health ergonomics legislation

regulations limits

NewsScan

## WORLD'S STRICTEST CELL PHONE RADIATION LAW? IN CHINA!

China, which is below international norms for most environmental standards, is considering strict new regulations that would cut cell phone radiation emissions by half of what they are overseas. The cost to cell phone makers would be enormous, because China represents such a huge market for cell phones and because manufacturers would have to redesign their entire operations, from R&D to production. Scientific studies have so far failed to find any evidence that cell phone emissions cause brain cancer, but the World Health Organization (WHO) has also said that further research is necessary before ruling out that possibility. (Reuters/USA Today 24 May 2002)

http://www.usatoday.com/life/cyber/tech/2002/05/24/china-cell-radiation.htm

## 26.2 Toxic materials

Category 26.2 Toxic materials

2002-05-10 ergonomics health hazards microbes germs workstations computers

NewsScan

## EEWWW! WORKSTATIONS ARE 'DIRTIER THAN TOILETS'

A study by University of Arizona microbiologist Chuck Gerba has revealed a "bacterial nightmare" lurking on the keyboards of the average computer workstation. Gerba's study, which swabbed keyboards, telephones and office lavatories and compared the bacterial count on each, showed the telephone as the worst offender, followed by the workstation, which had 400 times more bacteria than the average toilet. Unlike bathrooms, most workstations are rarely cleaned, says Gerba, leaving them the repositories for "millions of bacteria that could potentially cause illness." (vnunet.com 9 May 2002) http://www.vnunet.com/News/1131608

Category 26.2 Toxic materials

2002-09-27 toxic waste international shipping dumping

NewsScan

## CHINA REFUSES TO ACCEPT U.S. ELECTRONIC JUNK

Customs officials in China's Zhejiang province have said they will not accept receipt of 400 tons of electronic trash -- scrap computer monitors, keyboards, copiers and color TV sets -- that arrived two weeks ago and has sat unclaimed. The 22 containers, each 40 feet long, were marked "electronic products." "As the address and telephone number on the shipping bills are fake, we believe this is most likely a deliberate move to transfer electronic garbage," said one official. Such items are banned under Chinese law from entering the country, and the containers will be returned to where they came from, said the official. (AP 26 Sep 2002)

http://apnews.excite.com/article/20020926/D7M9K5BO0.htm

Category 26.2 Toxic materials

2002-10-28 toxic materials recycling

NewsScan

## PHONE RECYCLING GETS A BOOST

With more than 128 million cell phone users in the U.S. upgrading their handsets every 18 months on average, a record number of obsolete devices are hitting incinerators and landfills. That has environmentalists concerned because the phones contain toxins such as lead, cadmium and mercury that "accumulate in the environment and can cause damage to the ecosystem," says Eric Most, director of INFORM's Solid Waste Prevention Program. By 2005, INFORM predicts that 130 million cell phones weighing about 65,000 tons will be "retired" annually in the U.S. But now users have the option of donating their old phones to nonprofit groups or developing nations, or sending them off to be recycled in environmentally safe ways. "The simple act of recycling your cell phone can have profound ramifications," says Seth Heine, president of Collective Good (www.collectivegood.com), which runs a cell phone collection program. "The money can be used for immunization to keep a child from dying from a disease, or you can save 1,000 square feet of rain forest forever." People can also donate phones through www.donateaphone.com, operated by the Cellular Telecommunications and Internet Association's Wireless Foundation. Phones can be dropped off at Radio Shack, The Body Shop and Sprint PCS stores. (Reuters 26 Oct 2002) http://makeashorterlink.com/?V2D631342

Category 26.2 Toxic materials

2002-11-11 software disks waste toxic materials marketing protest

NewsScan

## DISK WAR

Two California men have been organizing a massive but polite attack on AOL for that company's distribution of promotional disks; they've established a Web site to encourage people to send them unwanted disks offering trial subscriptions to AOL's service, and when they have collected a million of the disks they'll haul them to the company's Virginia headquarters: "Basically, we'll enlist the help of volunteers who are willing to take a pickup load and drive back to AOL headquarters with us." Their hope is that the publicity stunt will demonstrate to the company that people consider its disk-distribution practices a waste of resources and a detriment to the environment. (AP/CNN Money 11 Nov 2002) http://money.cnn.com/2002/11/11/news/aol\_cds.ap/

# 27.1 Vulnerability assessment

Category 27.1 Vulnerability assessment

2002-01-22 financial security services outsourcing management

NewsScan; http://news.ft.com/news/industries/infotechnology

## IBM AND VERISIGN INK SECURITY ALLIANCE

IBM and VeriSign have established a global alliance to provide Internet security services to large corporations in a move that could generate more than \$1 billion over the next three years. VeriSign will use IBM's computer systems to run its future digital security services. Previously, VeriSign had used servers from Sun Microsystems. (Financial Times 22 Jan 2002)

Category 27.1 Vulnerability assessment

2002-01-24 security industry collaboration communications encryption services e-commerce

Security Wire Digest, http://www.ibm.com/news/us/2002/01/22.html

4 6

In January 2002, IBM and VeriSign announced a partnership to support a wide range of security services including "secure messaging, secure extranets, intranets and e-commerce sites, as well as secure document management." According to an article by Shawna McAlearney writing in Security Wire Digest, industry analysts saw the move as an aggressive push to take advantage of the two companies relative areas of expertise in support and in security technology to increase their market share in the security arena.

Category 27.1 Vulnerability assessment

2002-04-25 vulnerability analysis software quality assurance QA patches false positives

Security Wire Digest 4 32

The Microsoft Baseline Security Analyzer (MBSA) was released in early April 2002; by the end of the month, widespread reports indicated that the product was prone to excessive false positives, with many installed patches displayed as missing. Microsoft responded that they were aware of the problems.

# 27.4 Firewalls & other perimeter defenses

Category 27.4 Firewalls & other perimeter defenses

2002-01-20 firewall VPN DoS prevention content filtering

Security Wire Digest 4 5

## ZYXEL LAUNCHES THREE IPSEC VPN FIREWALLS

ZyXEL Communications, a manufacturer of firewall and broadband access devices, last week [January 2002] released three new firewall products—ZyWALL 1, ZyWALL 50 and ZyWALL 100. The products are scaled to allow home or business users to purchase a firewall with the exact number of VPN tunnels they require. ZyWALL offers stateful packet inspection, denial-of-service (DoS) attack prevention and Internet content filtering. http://www.zyxel.com

Category 27.4 Firewalls & other perimeter defenses

2002-03-14 firewall ISP Internet service provider interaction default disable denial-of-service

RISKS 21 98

Tim Loeb reported that connecting to the Earthlink ISP disables Windows XP's firewall without notification. This happens even though the firewall does work -- once -- immediately after being enabled. However, logging on to the network again immediately disables the firewall.

Category 27.4 Firewalls & other perimeter defenses

2002-04-25 firewall proxy servers US military DoD Department of Defense US Army

Security Wire Digest 4 32

## \*ARMY INSTALLS WEB PROXY SERVERS

The Army has set up proxy servers for its public Web sites to help prevent the actual sites from being attacked. The practice is common in the corporate world, where proxy servers allow public access to company information without providing crackers direct means to access the Web server. Gartner Group security analyst John Pescatore told Federal Computer Week that Web sites' susceptibility to defacement decreases from 67 percent to less than 5 percent with good application-level firewalls, which are similar to the proxy server system being used by Army sites. The server setup is part of a broader program called Web Risk Assessment Cell, created in 1999 to monitor Department of Defense Web sites and maintain the security of sensitive data accessible on public Web sites.

# 27.7 Anti-malware technology

Category 27.7 Anti-malware technology

2002-07-18 antivirus malware homeland defense

NewsScan

## BE PATRIOTIC -- UPDATE YOUR PC SECURITY SOFTWARE!

Keeping your home computer's anti-virus software isn't just good maintenance -- it's downright patriotic, says Richard Clarke, computer security adviser to President Bush. "Every American relies upon cyberspace and every American has to do something to secure their part of cyberspace," says Clarke, who's planning to unveil a national plan to protect cyberspace on Sept. 19. The plan, which is being hashed out among government officials with input from technology firms, will serve as the Internet component of the overall national strategy for homeland defense. It will include recommendations in five categories: home and small-business users; major corporations; "sectors" like banking, utilities and government; national issues; and global Internet users. (AP 17 Jul 2002)

http://apnews.excite.com/article/20020717/D7KQTBU80.htm

Category 27.7 Anti-malware technology

2002-11-01 adaptive response anti-malware quarantine database prototype

NewsScan

## SOFTWARE REPAIRS DAMAGE WHILE SYSTEMS WORK

Researchers at Pennsylvania State University have developed software that can quarantine malicious commands and repair any damage that's been done to a system, while the database continues to process transactions. "We can't prevent attackers from getting in, but with this technology, the database can heal itself on the fly? The database can adapt its own behavior and reconfigure itself based on the attack," says Dr. Peng Liu, who heads up the Penn State team. The Cyber Security Group and the U.S. Air Force are testing a prototype of the software, which is not yet commercially available. Several large database vendors have begun offering self-healing systems, but analysts say the Penn State effort is the most advanced so far. "There are various tools that can detect anomalies, but they simply generate a report or display that calls someone's attention to it," says an IDC analyst. "The interesting part of the (Penn State) research? is the ability to automatically respond to the attack." (CNet News.com 31 Oct 2002)

http://news.com.com/2100-1001-964109.html?tag=fd\_top

Category 27.7 Anti-malware technology

2002-11-26 antimalware control bandwidth reduction throttle limitation spread response time worm e-mail

NewsScan

## ANTIVIRUS TOOL THROTTLES DOWN ON INFECTION RATE

Matthew Williamson, a researcher at the Hewlett-Packard labs in the UK, has developed a new approach to battling computer viruses. It slows down the infection rate significantly by limiting the number of connections at any one time by an infected computer. "The major problem with computer viruses is that because they spread so quickly and our response is so slow, they cause so much damage," says Williamson. "We are tackling the fundamental nature of a virus? When your machine gets an email virus, it sends lots and lots of e-mail messages at a much higher rate than you would normally send them. So if I put a limit on the rate of e-mail messages that you can send in every 10 minutes, then a virus trying to send 100 or 200 messages will very quickly get delayed." Williamson found that using the "throttle" technique has a negligible impact on the day-to-day performance of his computer. (BBC News 26 Nov 2002)

http://news.bbc.co.uk/1/hi/technology/2511961.stm

# 28.1 Spyware & cookies

Category 28.1 Spyware & cookies

2002-04-06 HTML e-mail Web bugs spyware firewalls browsers configuration adware cookies

RISKS 22 03

Stefanie Olsen, writing for CNET News, noted the rising concern over the use of HTML e-mail containing spyware such as Web bugs -- 1-pixel invisible images that reside on Web sites where counters keep track of who is downloading them, thus keeping a record of the success of spam campaigns.

[MK comment: most personal firewalls (e.g., ZoneAlarm) and some browsers (e.g., Opera) allow configuration that stops downloads of materials from outside a target Web site, thus interfering with adware and spyware.]

Category 28.1 Spyware & cookies

2002-06-27 spyware communication firewall instant messaging chat

RISKS 22 13

Michael Weiner reported, "Since I installed MS Messenger 4.6 (4.6.0082) on my machine, my firewall is going wild: In addition to numerous Microsoft sites, Messenger is contacting the following sites each time I log in: expedia.com, xp.mcafee.com, carpoint.msn.com and port-64-1956779-zzt0prespect.devices.datareturn.net. No way to know what information MS Messenger is transmitting to these sites, I did not find any meaningful information on it on the Microsoft website..."

Category 28.1 Spyware & cookies

2002-10-14 P3P Platform for Privacy Preferences W3C standards proprietary implementation

browsers developers

#### NewsScan

## THE COLORS OF PRIVACY

Be careful what you ask for: you may just get it (more or less). Privacy advocates put continuous pressure on Microsoft to pay careful attention to privacy concerns, but many Web publishers are now unhappy with Microsoft's implementation of the Internet Explorer 6.0 browser, which seeks to discourage third-party tracking abuses by blocking third-party "cookies" unless the third party's privacy policy meets strict standards. Third parties are required to put their policy into the P3P ("platform for privacy preferences") protocol specified by the World Wide Web Consortium, but there are vastly different levels of compliance with that standard, and there is worry that publishers will put a great deal of work into complying with Explorer's implementation of the standard, and then learn that Microsoft has decided to change the standard with the next software release. Carl Fischer of iVillage says, "Our legal department has been working on this for months. And Microsoft can just change its standards down the line. They're imposing a one-size-fits-all rule for hundreds of different privacy policies. Why should that be up to Microsoft?" (New York Times 14 Oct 2002)

## 28.2 Scumware

Category 28.2 Scumware

2002-01-04 spyware music-sharing peer-to-peer unauthorized installation implementation supervision QA quality assurance

NewsScan

## USER WEB HABITS TRACKED BY SOME MUSIC-SWAPPING PROGRAMS

The Web surfing habits of people who used the LimeWire, Grokster and KaZaA music-sharing programs were surreptitiously tracked because those programs were linked to an online sweepstakes game called ClickTillUWin, in which players pick numbers and win cash prizes. The company that operates the sweepstakes game says it told outside distributors to get users' permission before installing the software, but in these cases that action was not taken. The three companies have posted new versions of their software without the tracking component, and LimeWire has issued an apology. (AP/USA Today, 4 Jan 2002) http://www.usatoday.com/life/cyber/tech/2002/01/04/limewire-tracking.htm

Category 28.2 Scumware

2002-01-11 scumware Lotus Notes unauthorized undocumented data modification corruption

diddling arrogance stupidity criminal negligence design flaw bug error expletive deleted

RISKS 21 88

Erling Kristiansen posted a note in RISKS discussing undocumented, unannounced data loss in Lotus Notes. The author's examples follow verbatim:

- \* I printed a mail message before I sent it. Some of the cc: addresses were quietly and permanently removed. (Did anybody say buffer overflow recently? Maybe it is more like buffer truncation, but certainly member of the same family)
- \* Trying to reply to a mail I received, I discovered that 3 out of the about 10 cc: addresses in the incoming message had been truncated, rendering them invalid. No addresses were lost completely, but the amount of truncation that occurred suggests that a short address might be "truncated into extinction" if it is in the right place in the list of addresses. I checked the original RFC-822 header that is accessible. It was correct.

By the way, correcting the addresses in place and re-sending had a very strange effect: The corrected addresses, and only those, were turned into an X.400-like address with a number of attributes pointing to my local environment. I had to remove and retype the "sick" addresses to have them accepted.

- \* I copied and pasted about 100 addresses from a spreadsheet into the bcc: field of a mail. Everything looked OK, the pasted addresses appeared neatly in the address window, I could scroll through them, etc. But the message was only sent to the first address. No warning of any kind appeared that a good hundred addresses had been discarded. I only discovered the error because I had asked for delivery notification, and got very few. Had I not discovered this, only a handful of people would have been invited to a presentation. (there were a few other addressees that had not been pasted in those worked OK even though some were entered AFTER the skipped addresses).
- \* Notes allows you to format messages, with facilities more or less equivalent to an HTML editor. If a message is sent outside the Notes domain, ALL formatting is removed, even things like indentation and paragraph numbers. So a nicely formatted message may become rather unreadable, even ambiguous (indentation may imply a lot about the meaning of a text). No warning is given that formatting information is being removed.

The RISKS correspondent concludes, "The RISK of all this is that Notes accepts instructions to do something, does not complain about the input, and then goes ahead and does something else than what could reasonably be expected. You can obviously check for any of these events, but they are rare enough, and different enough, that you don't really know when to expect a problem, and what to look for in order to make sure everything went as expected."

Category 28.2 Scumware

2002-01-18 scumware Microsoft Excel unauthorized undocumented data modification

corruption diddling arrogance stupidity criminal negligence design flaw bug error expletive deleted

RISKS 21 88

Geoffrey Brent, writing in RISKS, identified yet another Microsoft undocumented, unauthorized data modification. If you open two MS-Excel files and copy a cell containing a number and paste it into a cell in the other file, everything works fine. For example, 1.2345 gets copied as 1.2345 regardless of how many figures are showing in the cell. However, if you open file A, copy a number, \_close file A\_, and then paste the number into file B, you get a value that is identical to what was \_visible\_ rather than to what was entered in the original cell. Thus in the example above, 1.2345 in the source becomes 1.23 in the destination worksheet. [MK note: I tested this myself in Excel 2000 and it's true.]

Category 28.2 Scumware

2002-01-28 scumwarescumware unauthorized modification editing changes invisible data

corruption integrity arrogance word processing spreadsheet office software design

flaw arrogant public relations dismissive

RISKS 21 90

Bear Giles reported that Microsoft Outlook has an erroneous algorithm for recognizing UUENCODED text within the body of a message. The designers incorrectly assumed that any line beginning with the word "begin" must be the start of UUENCODED text. The algorithm does not bother to check for any other evidence that this assumption is correct, with the result that perfectly ordinary text is relegated to an attachment and may easily be lost. In addition, malware writers have already figured out that they can send ordinary text messages and have Outlook obligingly convert embedded malicious code into an attachment \_after\_ it has gone through a firewall or e-mail filtereven if users don't permit attachments to get through.

Microsoft's breathtakingly arrogant workaround (not solution) for their own design error was to recommend that everyone on the planet either stop using the word "begin" or use the capitalized form "Begin" in all e-mail messages sent to Outlook users or potentially forwarded to Outlook users -- that is, in effect, in all e-mail messages the world over.

Category 28.2 Scumware

2002-01-29 scumware automated spelling correction software

RISKS 21 90

Automated spelling-correction software mangled several names in the HP annual report; examples include "David and Lucite Packard Foundation" [from "Lucile"], "Edwin van Pronghorns" [from "Bronkhorst], "Eleanor Hewlett Limon" [from "Gimon"], and "Mary Hewlett Gaffe" [from "Jaffe"].

http://www.siliconvalley.com/docs/news/tech/085146.htm

Category 28.2 Scumware

2002-02-12 scumware Google search engine periods removed data modification corruption email address bounce

RISKS 21 91

Google appears to remove some periods even in e-mail addresses that appear in the summary lines for hits. Robert Marshall reported this problem to RISKS as follows (quoting verbatim):

I was searching for the work e-mail address for a friend using google. Let's say the name was Paul Consultant. Google gave me a hit with the correct company and the web page was such that his e-mail appeared in the google summary. So I cut and pasted it directly without having to visit the company web site. It appeared as PR.Consultant@relations.com.

When the e-mail bounced I investigated and the company web page has the mail as P.R.Consultant@relations.com, as does google's cache. It looks as if google is trying to cut down on the synposis by removing redundant '.'s

Unfortunately they aren't always redundant. Fortunately my e-mail bounced rather than going to an unrelated recipient.

Category 28.2 Scumware

2002-03-05 privacy spyware redirection search engine privacy monitoring surveillance

RISKS 21 93

Sim IJskes found that even though he reconfigured Netscape browser v6.2 to use GOOGLE instead of the netscape.com search engine, in fact the product shunted his requests through their search engine before passing the search on to GOOGLE. Commented the correspondent, "I guess that Netscape allows you to search other search engines than their own, but still wants to know what you are searching...."

Category 28.2 Scumware

2002-04-25 **P2P** peer-to-peer Trojan distributed processing reverse engineering

Security Wire Digest 4 32

## \*KAZAA CRITICIZED FOR SECONDARY SOFTWARE

Since peer-to-peer file sharing service KaZaa came under fire for surreptitiously including secondary software with every download, a Russian hacker has created a "KaZaa Lite" version sans a program that allows a third party to tap into a user's computer processing power and storage space. KaZaa owner Sharman Network has not said what actions, if any, it will pursue against Russian programmer "Yuri" and Kazaalite.com, which has processed more than 80,000 downloads since its release earlier this month, according to a published report. Sharman quietly has been installing software in KaZaa downloads that could allow a secondary file-swapping network called "AltNet" to draw upon users' resources for use in distributed computing. KaZaa estimates that about 20 million users have the software installed on their machines. Several media reports have said the secondary software works the same as a Trojan. The company has since changed its user agreement policy.

# 28.3 Keystroke loggers

Category 28.3 Keystroke loggers

2002-06-26 keylogger Trojan confidentiality eavedropping data leakage espionage organized

crime password user ID college university students

## NewsScan

## RUSSIAN MOB TARGETS SOME U.S. COLLEGE COMPUTER SYSTEMS

A Russian-born man at Pasadena City College has been arrested as he tried to install keystroke-recording software to capture student credit card information, and Arizona State University officials found that a program had been surreptitiously installed to steal student credit card numbers, passwords, and e-mail. Linking these and other activities to Russian organized crime, the Secret Service and the Education Department have joined in issuing a general alert to American college computer centers. (AP/USA Today 26 Jun 2002)

http://www.usatoday.com/life/cyber/tech/2002/06/26/college-computers.htm

# 29.1 Addiction

Category 29.1 Addiction

2002-02-26 online sex cybersex addiction survey

NewsScan

#### ADDICTED TO "ADULT" SITES

An online survey by the San Jose Marital and Sexuality Centre reports that 10% of the 7,037 individuals responding to the survey say they are addicted to cybersex. Other data: Neilsen/NetRatings figures indicate that there were 27.5 million U.S. visitors to adult-oriented sites last month; of that number, 72% were men and 28% women. (USA Today 25 Feb 2002) http://www.usatoday.com/life/cyber/tech/2002/02/26/cybersex.htm

Category 29.1 Addiction

2002-07-01 electronic auction fanatics fans addicts enthusiasts groupies

NewsScan

#### EBAY BELIEVERS IN LOVE WITH MEG

Online auctioneer eBay now has 50,000 million customers, a great many of whom don't think of themselves as customers at all, but as entrepreneurs, pioneers, and friends. They honor Pierre Omidyar, who founded the company in 1995, and are in love with Meg Whiman, eBay's billionaire chief executive officer. Marketing professor Eugene Fram of Rochester Institute of Technology explains: "These are innovation junkies -- like the people who used to follow the Grateful Dead around the country. Every day, fifty thousand new people participate in eBay auctions, and the company insists that, despite the fears of skeptics, eBay will never let its search for corporate customers interfere with its commitment to individual buyers and sellers, who built the company's success and who continue to generate excitement for its mission." At a recent convention of 5,500 eBay lovers, one eBay junkie enthused: "It's like a reunion of people you've never met." (USA Today 30 Jun 2002) http://www.usatoday.com/life/cyber/2002/07/01/ebay.htm

Category 29.1 Addiction

2002-08-23 Internet addiction survey study

NewsScan

# ONE IN FOUR U.S. WORKERS ADDICTED TO THE NET

Twenty-five percent of U.S. employees report that they are addicted to going online, according to a survey conducted by Websense, although only 8% of companies polled report any knowledge of workplace Internet addiction. According the report, these workers spend more than one entire workday each week accessing non-work-related Web sites. The top five types of sites labeled most addictive were: shopping, news, pornography, gambling and online auctions. The study reports that while 78% of workplaces have installed filters to prevent employees from accessing pornography while at work, only 47% block access to gambling sites. Employers are generally reluctant to block access to news sites, with only 4% reporting they had done so. (Nua Internet Surveys 22 Aug 2002)

Category 29.1 Addiction

2002-09-24 Internet addiction work policies acceptable use survey

NewsScan

# NEWS SITES SERVE UP 'ADDICTIVE' CONTENT

Workers who surf on the job report that they visit online news sites more often than pornography, gambling, or even online auction sites, and that they consider news one of the most addictive types of content available on the Web, according to a survey by Websense. "Initially we saw the most abuse in pornography and gambling sites, now we are seeing more time spent on shopping and news sites," says Websense CTO Harold Kester. Twenty-three percent of those surveyed cited news as the most addictive Web content, compared with 24% who chose shopping, 18% who picked pornography, 8% for gambling and 6% for online auctions. Meanwhile, employers don't seem too perturbed over their workers' penchant for current events. Sixty-seven percent said there were no restrictions in the office on reading news online. That compared with 37% who allowed access to shopping and auction sites, and a slim 2% who didn't mind if their employees visited gambling and porn sites while on the clock. Workers reported spending 8.3 hours a week -- 20% of their worktime -- on Internet sites that had no relation to their jobs, and most said they would rather give up coffee than the Internet. (Reuters/CNN.com 23 Sep 2002)

# 29.2 Cybersyndromes

Category 29.2 Cybersyndromes

2002-09-03 sociology pathology games role-playing online harassment anti-social behavior

NewsScan

#### GRIEFERS RELISH THE DARK SIDE OF CAMELOT

Griefers -- online game players who focus on the indiscriminate slaughter and ridicule of other gamers -- have caught the attention of game makers such as Sony, Microsoft and Electronic Arts, who worry that these bad sports will jeopardize the rise of online games by scaring away customers willing to spend \$10 to \$14 a month to subscribe to the online gaming experience offered by titles such as "EverQuest" and "Dark Ages of Camelot." These games offer players rich, immersive, fantasy worlds where they can acquire virtual jobs, adopt pets, marry and own property. Rather than a shining city on a hill, however, the online Camelot has quickly descended into anarchy, where stealing, killing, taunting and other forms of bullying are used to torment novice players. For a griefer, this is what it's all about -- not the killing, but the misery they inflict afterward. "Griefers feed on the negative reactions of the people they kill," says one self-proclaimed bully. "There's nothing sweeter than when you kill someone and they spout insults at you for hours. That's when you know you got him. It sounds really cruel, but it's fun." And while game makers have tried to isolate anti-social behavior by setting up safe zones where players can't be harmed and filters that reject obscene and graphic names, the griefers continually find ingenious ways to get around them. The result is a cat-and-mouse game that has become tremendously costly for game developers at the same time they are planning to significantly expand their online offerings. "We're trying to take a whole new generation of players online who have never been there before," says the director of content services for Microsoft's Xbox. "We want to make sure everyone has a good experience." The griefer's response? "Everybody needs a bad guy." (Los Angeles Times 2 Sep 2002)

Category 29.2 Cybersyndromes

2002-12-11 Internet browsing searching male chauvinism sexism

NewsScan

#### BATTLE OF THE SEXES MOVES TO CYBERSPACE

A survey conducted by search engine AltaVista reveals that male chauvinism is alive and well on the Internet, with 80% of men polled claiming to be better at Web surfing than their female counterparts. Men also admit to being backseat drivers, interfering with their partners while they try to surf the Web, and of those who experienced the impatience and frustration of "Net rage," two-thirds were men. "As information has become such a valuable commodity, it's not surprising that men have transferred their traditional hunter-gatherer role to hunting for information on the Web," says Open University psychologist Dr. Adam Joinson, who adds it's unlikely that men actually are better at Web surfing than women. "I'd be surprised if men's self-perceived superiority is grounded in fact." (BBC News 11 Dec 200) http://news.bbc.co.uk/1/hi/technology/2562601.stm

# 29.3 Digital divide

Category 29.3 Digital divide

2002-07-05 digital divide international Linux personal computer PC Internet

NewsScan

#### INDIA'S CHEAP NEW HANDHELD "SIMPUTER"

India's new "Simputer" -- a handheld computer whose name was chosen to suggest that it is simple, inexpensive, and multilingual -- will cost between 10,500 to 23,000 rupees (\$214-469), in a country where the average per capita income is about \$450. Using a Linux operating system, the device will have applications for voicemail, text-to-speech translation, and Internet access, and will be powered by an Intel StrongARM processor and two AA batteries. Random-access memory options will be 32 or 64 megabytes. The Simputer was designed by engineers at Encore Software and professors from the Indian Institute of Science in Bangalore, and will be marketed through a few large Indian technology companies. (Reuters/San Jose Mercury News 5 Iul 2002)

http://www.siliconvalley.com/mld/siliconvalley/3605609

Category 29.3 Digital divide

2002-07-18 digital divide children access power international

NewsScan

#### WHEN YOU COME TO A DIGITAL DIVIDE, LEAP OVER IT

And how do you do leap over the digital divide? By concentrating not so much on computer literacy -- but rather on computer power. In 1993, with money from Intel, MIT Media Lab professor Mitchel Resnick helped establish the first site of what is now an international network of 50 Computer Clubhouses, which are places where boys and girls 8 to 18 can "really feel in charge of the technology." Resnick says, "Access is not enough. Access is just a starting point. It's not about playing games, but about making your own games. It's not about surfing the Web, but it's about making your own Web pages. It's not just about downloading MP3 music files, but doing your own music composition." The clubhouse network has a \$32 million commitment from Intel through 2005, in addition to hardware, software and services donated from Adobe, Macromedia, HP, Autodesk, and other companies. The network extends throughout the world, and includes such countries as Ireland, Israel, India, Germany, the Netherlands, and the Philippines. (New York Times 18 Jul 2002)

Category 29.3 Digital divide

2002-07-23 digital divide international usage survey study

NewsScan

# CHINA IS NO. 3 IN INTERNET USERS

Exceptionally strong growth in Internet use over the past year has vaulted China to the No. 3 position in the world in terms of online population numbers. A 72% increase since last year translates to 45 million Chinese citizens now logging on regularly, even as the government still struggles with how to control subversive content. Only the U.S. and Japan have more citizens online, according to a report from the China Internet Network Information Center, an industry group funded by the Information Industry Ministry. The average Chinese user spends eight hours and 20 minutes online each week, and while Internet formerly was concentrated among academics, 68% of current users do not have college degrees. "The Internet is now coming closer to common people," says the People's Daily newspaper. (AP 23 Jul 2002) http://apnews.excite.com/article/20020723/D7KUIAUG1.htm

Category 29.3 Digital divide

2002-08-27 digital divide international access

NewsScan

#### HINDI CHATBOT OPENS INTERNET TO MILLIONS

Computer science students in India have developed an interactive software program fluent in Hindi that could demystify computers for millions of Indian citizens. "The good thing about Deepti [the program] is that it is suitable for the Indian environment," says Ritvik Sahajpal, one of the students who worked on the program. "Deepti speaks in Hindi and since the majority of the people in India are computer illiterate and don't speak English, this feature is really great." The students say Deepti could be used to make government services more accessible, or it could be linked with touchscreen technology so that people with little or no knowledge of computers could use Internet kiosks. (BBC News 27 Aug 2002) http://news.bbc.co.uk/1/hi/technology/2209775.stm

Category 29.3 Digital divide

2002-09-04 digital divide international technology telecommunications Internet Africa report

#### NewsScan

NewsScan editors John Gehl and Suzanne Douglas published an interesting report from their special correspondent Wilcliff Sakala, who is based in Zambia, on information technology in Africa. Some highlights:

- \* Africa is progressing on the road to integrate Information and Communication Technologies.
- \* In East Africa, the IT market value is set to expand at a compound annual growth rate (CAGR) of 21 per cent between 2000 and 2004.
- \* Tanzania will lead the growth rate in East Africa, with a forecast 28 per cent (\$135 million) CAGR by 2004.
- \* Uganda will follow, registering a 25 per cent CAGR in the same period, totaling \$63 million.
- \* Since 1991, telephone penetration in Least Developed Countries (LDCs) has risen from 0.3 to 1.1 per 100 people.
- \* Nigeria is drastically expanding its telecommunications infrastructure with the development of a more democratic government.
- \* Zimbabwe's three cellular providers have a subscriber base of more than 300,000, and the private operators have more lines than the State's fixed phone network.
- \* South Africa has the largest number of Internet subscribers in Africa, accounting for more than 80 per cent of the continent's estimated 2.6 million Internet users.
- \* Poverty presents another big challenge towards efforts to provide communication facilities to the majority of people in Africa. Innovative products include pre-paid packages, and phone shops that services previously under-serviced high-density and rural areas.
- \* Since 2000, Tunisia's mobile penetration has more than tripled, recording 4.01 per cent at the end of 2001 from 1.2 per cent. Meantime, mobile phone subscribers rose from 119,075 in 2000 to 404,202 by March, 2002.
- \* In Kenya, it is the tourism and non-traditional sectors, such as horticulture, that are driving e-commerce. A 1999 study by Kenya Association of Tour Operators showed that 10 per cent of membership had an Internet presence and conducted business on-line.

Category 29.3 Digital divide

2002-09-24 broadband cable access digital divide ISP Internet service provider survey

#### NewsScan

#### BROADBAND'S AVAILABLE, BUT HAS FEW TAKERS

Almost every U.S. household has potential access to a high-speed Internet connection, but only 10% subscribe to such a service, lower than the rate in Taiwan, South Korea, Hong Kong or Canada. About half of U.S. families have some type of Internet access at home. A report from the U.S. Commerce Department's Office of Technology Policy cites a need for more compelling content in order to boost the adoption of broadband: "New applications and services that consumers want and businesses need will provide the tipping point for broadband demand and usage." The report credits Napster, along with PCs, CD-ROM writers and larger hard drives, for promoting the use of broadband access. Along with lack of content, the report says the relatively high cost of high-speed access is another obstacle to wider usage. Broadband access costs about \$50 a month vs. \$20 a month for dialup connections. An August 2002 Yankee Group survey indicated that more than 70% of dialup users cited cost as the main barrier toward upgrading to faster access. (AP 23 Sep 2002) http://apnews.excite.com/article/20020923/D7M7GVS00.htm

# Online voting 29.4

Category 29.4 Online voting

2002-01-09 cybercourt Internet connection legal system vulnerabilities interception man-in-the-

middle attack confidentiality reliability availability integrity data diddling

#### NewsScan

#### MICHIGAN GOVERNOR ESTABLISHES CYBERCOURT

Michigan Governor John Engler has signed into law a bill to create a virtual state court -- the first to operate in the U.S., according to Matt Resch, an Engler spokesman. A cybercourt exists at the College of William and Mary in Virginia, but isn't operational, says Resch. The court won't have a jury and will handle only business disputes involving at least \$25,000. District or circuit court judges will be assigned for three-year terms and will be specially trained to use the system. "In a world where we can go from idea to IPO at warp speed, we need a connected court that can keep up," says Engler. (AP 9 Jan 2002) http://apnews.excite.com/article/20020109/D7GU9I300.html

Category 29.4 Online voting

2002-01-19 Web voting fraud ballot stuffing automation reliability

RISKS 87 21

News reports about an unscientific poll about preferences between Java and Microsoft's .NET indicated that some Microsoft employees were "trying to vote repeatedly, including automated voting."

MORAL: don't trust the results of Web-based polls that use self-selected respondents and weak anti-fraud controls.

Category 29.4 Online voting

2002-01-26 online court proceedings judgements Web

RISKS 21 89

Tony Ford summarized a new official self-service litigation system available in England & Wales in a brief article in RISKS (quoted verbatim below):

Today's Daily Telegraph (a quality UK broadsheet newspaper) carries a \*potentially\* disturbing report describing a new service, "Money Claim Online", whereby individuals and law firms (solicitors) can issue most simple legal proceedings (where a sum less than UK pounds 100,000 is claimed, = USD 140K)) and enforce judgments via a Web browser. The new service has been set up without publicity by the Lord Chancellor's Department, which runs the courts system in England and Wales. It seems that the system is accessible to the public now, although it has not been officially launched.

People using the service are (oddly) referred to as "customers" .... and there is a Customer Help Desk ...

The newspaper report is also viewable at this Daily Telegraph link on-line:

http://www.telegraph.co.uk/news/main.jhtml?xml=/news/2002/01/26/nsue26.xml&sSheet=/news/2002/01/26/ixhome.ht ml

The service can be seen on-line at: https://www.moneyclaim.gov.uk/csmco/index.html

No details are apparent of what measures are taken to validate the identity of the claiming party or prevent other gross miscarriages of justice .... but it would appear that the potential exists for significant trouble .... even though the site warns that "vexatious litigants" are not allowed to us it (these are people who have abused the litigation system in the past to such an extent that they have been declared "vexatious litigants", restricting their ability freely to issue legal proceedings).

PS: I am a lawyer myself, although I don't practise in this area .. but do work in-house for a large IT company ... these comments are offered purely in a personal capacity.

Category 29.4 Online voting

RISKS

2002-01-30 online voting touchscreen COTS insider fraud penetration intrusion audit trail tampering data diddling QA quality assurance

21 90

David E. Price reported that "officials in Florida's Miami-Dade County have approved a \$24.5 million contract to replace the county's punch-card voting system with touchscreen equipment, in time for Nov 2002. The touchscreen machines make it impossible to vote for more than one candidate in each race, known as overvoting, and alert voters if they fail to select any candidate, or undervote. Two other counties that were at the heart of the controversy -- Palm Beach and Broward -- also plan to use touchscreens."

Peter G. Neumann added, "And as we have noted here before, today's touchscreen systems provide essentially ZERO hard evidence that your vote is counted as cast, and not for someone else or for no one. With just a little insider fraud, what a remarkable opportunity for rigging elections!"

A couple of weeks later, Alan Brain added the following concise commentary:

"The risks for vote-rigging on COTS systems [include]:

- a) Someone tweaks the BIOS of the voting machines. b) Someone tweaks the OS of the voting machines. c) Someone tweaks the applications code d) Someone tweaks the compiler.
- a) Can best be dealt with via physical security only have non-flashable BIOSes, and disallow unauthorised access.

The rest require both a publicly available Open Source codebase, and physical security to make sure that what you think is on the machine, actually is. And that the right OS has been installed, and the right compiler used."

He added, "Conversely, if the voting is being done with machines where the OS, Applications Sourcecode and Compiler aren't Open Source, then security is problematic."

Category 29.4 Online voting

2002-02-20 onnline voting fraud countermeasures COTS commercial off-the-shelf software

RISKS 21 92 FF

The RISKS Forum was the locus of a vigorous discussion of online voting hazards. The following collates contributions from various contributors:

[Alan Brain] The risks for vote-rigging on COTS systems [include]:

- a) Someone tweaks the BIOS of the voting machines.
- b) Someone tweaks the OS of the voting machines.
- c) Someone tweaks the applications code
- d) Someone tweaks the compiler.
- e) Someone tweaks the compiler of the compiler of the .... [Mike Nelson]
- a) Can best be dealt with via physical security only have non-flashable BIOSes, and disallow unauthorised access.

The rest require both a publicly available Open Source codebase, and physical security to make sure that what you think is on the machine, actually is. And that the right OS has been installed, and the right compiler used.

[Lee Barstow] With physical access to voting machines and/or the software used to control them, the only sure way to provide security is a paper record.

Especially with OpenSource software, it becomes possible to recompile (and hence alter) any electronic-only record. Closed Source software isn't any better - it lacks public accountability and scrutiny. Someone could always create a new ROM, OS, or software image if given sufficient knowledge, bypassing any security system that has been put in place.

So: Print an OCR paper record when the voter finishes his vote. He gets to check the paper copy and put it in a standard secured voting box. The best parts are:

- (a) Since it's printed on demand, only the voter's candidate appears on the printout the voter sees only who or what he voted for, or that he made no vote, and can easily check the paper before dropping it in the box.
- (b) Using OCR, independent auditing becomes easy. The auditor needs little in the way of custom hardware or software to do the job; they only need to tweak their OCR readers. Auditors could be chosen by mutual agreement of the candidates after the vote is completed (and only if a candidate determines he wants to have a recount), removing any temptation to bribe the auditing firm.

Category 29.4 Online voting

2002-04-22 online Web voting UK browsers identification authentication I&A interception

RISKS 22 04

In the English boroughs of Crewe & Nantwich in Cheshire, a couple of wards experimented with Web-based voting. The security measures consisted of sending two separate "secret codes" by two postal mailings to registered voters, who would then have to use either MS-IE or Netscape Navigator -- but only in the Windows versions. No other operating system versions need apply.

[MK comment: Hmm, talk about the digital divide...]

Category 29.4 Online voting

2002-04-29 online voting fraud criminal hackers penetration tampering corruption interference

NewsScan; http://www.washingtonpost.com/wp-dyn/articles/A64981-2002Apr29.html

# VIVENDI SUSPECTS ELECTRONIC VOTE FRAUD

Vivendi Universal, the Paris-based media giant, is calling for a criminal investigation of suspected fraud by unnamed computer hackers during a shareholders vote by Internet last week. Vivendi thinks the vote tampering "could have been carried out by a small team armed with a transmitter-receiver and detailed knowledge of the procedures and technical protocols of electronic voting." (AP/Washington Post 29 Apr 2002)

Category 29.4 Online voting

2002-05-16 online voting corporations companies industry postage Web

NewsScan

#### TREND TOWARD ELECTRONIC VOTING

More and more companies are allowing shareholders the option of Internet voting, motivated as much by reductions in postage costs as anything else. Mary Ann Butera of ADP Investor Communication Services says an Internet vote costs a company only about 3 cents, compared to a paper proxy which costs a company 34 cents. "It doesn't sound like much, because you're talking about pennies. When you multiply that over thousands of investors, it does add up." And of course there's the matter of pride of being on top of technology developments. Tom Newston of EquiServe notes: "A small company that only has hundreds of shareholders, or a few thousand shareholders, may not see the cost savings as a big number. But at the same time, they may want to be thought of as a forward-thinking, cutting-edge company." In the U.S., 85% use "traditional" voting methods: 70% of proxy voters mail their votes and 15% use the phone. (Tampa Tribune/San Jose Mercury News 15 May 2002) http://www.siliconvalley.com/mld/siliconvalley/3271361.htm

# 29.5 Online legal proceedings

Category 29.5 Online legal proceedings

2002-03-22 electronic legal notice anonymity e-mail legal judgement online gambling

NewsScan

#### COMING TO YOUR IN-BOX: "YOU'VE GOT A SUBPOENA"

A federal appellate court has ruled that a Las Vegas casino suing an unlocatable Internet gambling group can use e-mail to send sufficient notification of the legal action it is taking. Law professor Ann McGinley of UNLV says the decision sets a precedent that will "make it easier for lawyers to find elusive defendants. I think we are moving in the direction of service by e-mail." (AP/San Jose Mercury News 22 Mar 2002)

http://www.siliconvalley.com/mld/siliconvalley/2913542.htm

Category 29.5 Online legal proceedings

2002-09-30 e-mail legal proceedings traffic tickets court explanations

NewsScan

#### E-MAIL IT TO THE JUDGE

County officials in Yakima, Washington, are setting up a program that will enable citizens who've received traffic tickets to e-mail their explanations and excuses to a judge rather than sit in traffic court for hours waiting their turn. Judges will then have a choice of e-mailing their replies or responding via old-fashioned postcard. (AP 29 Sep 2002) http://apnews.excite.com/article/20020929/D7MBH7NG0.htm

# Surveys, studies, audits of security 31.1

Category 31.1 Surveys, studies, audits of security

2002-01-10 copyright intellectual property music sales statistics survey study royalties fees

NewsScan

#### LET THERE BE MUSIC, LET THERE BE LOVE, LET THERE BE VULGAR ROYALTIES

Soundscan, a company that tabulates retail sales of recorded music, has reported that the number of albums sold last year dropped 2.8% from previous-year's sales, the first decline since the company began a decade ago. One record company executive warns, "We have to rethink our business, and it may not be the record business anymore." Concurring with that assessment, Michigan congressman John Conyers Jr., the senior Democrat on the House Judiciary Committee, says: "Technology is forcing the record labels and the artists and the writers and the composers to come together. The Internet says to the industry that you folks are yesterday's news, you're following outdated models, your business strategies don't work anymore, and your profit motive is showing rather vulgarly." And Eben Moglen, a Columbia University law professor and general counsel of the Free Software Foundation, pleads for a return to the spirit of "music before Edison" -- a time when (he believes) music was not a commodity but a form of love. Alluding to the music-swapping experiments that take place on the Internet, Moglen argues that "everything that can be shared will be shared. But people make music because they love it, and they'll pay for it because they love it." (New York Times 10 Jan 2002) http://partners.nytimes.com/2002/01/10/arts/music/10CONF.html

Category 31.1 Surveys, studies, audits of security

2002-01-30 non-profit organizations security practices survey audit results sensitive data confidentiality intrusion vulnerability disaster recovery

RISKS 91

Audrie Kraus, Executive Director of NetAction, summarized the disturbing results of that organization's "survey of security practices in nonprofit organizations" which found among many other things that non-profits studied had "... substantial room for improvement, especially in maintaining the security of confidential and/or sensitive files, user work habits, and disaster planning."

http://netaction.org/security/.

Category 31.1 Surveys, studies, audits of security

2002-02-04 security industry survey study statistics revenue growth

NewsScan

#### SECURITY FIRMS PROSPERING UNDER NEW CONDITIONS

Computer security companies are surviving the technological recession quite nicely, and one of them, Symantec, expects to break the billion-dollar sales mark this year. Gartner says that Symantec is the No. 1 provider of security and antivirus software but that it has been trailing Internet Security Systems and Check Point Software Technologies in detection and firewall software. (San Jose Mercury News 4 Feb 2002)

http://www.siliconvalley.com/docs/news/svfront/symant020402.htm

Category 31.1 Surveys, studies, audits of security

2002-02-25 music piracy copyright intellectual property theft survey study statistics losses

damage ethics

## NewsScan

# RIAA: PUT ANOTHER NICKEL IN THAT NICKELODEON FOR MUSIC, MUSIC, MUSIC

The music industry is desperate to find a way of downloading a solution to the problem of illegal downloading of copyrighted songs. The Recording Industry Association of America (RIAA) says that shipments by record companies to consumers have dropped by more than 10% in the past year, and RIAA president Hilary Rosen complains: "When 23% of surveyed music consumers say they are not buying more music because they are downloading or copying their music for free, we cannot ignore the impact on the marketplace. " (Reuters/New York Times 25 Feb 2002) http://partners.nytimes.com/reuters/technology/tech-leisure-music.html

Category 31.1 Surveys, studies, audits of security

2002-02-25 online pornography addiction survey study statistics estimates

NewsScan

#### ADDICTED TO "ADULT" SITES

An online survey by the San Jose Marital and Sexuality Centre reports that 10% of the 7,037 individuals responding to the survey say they are addicted to cybersex. Other data: Neilsen/NetRatings figures indicate that there were 27.5 million U.S. visitors to adult-oriented sites last month; of that number, 72% were men and 28% women. (USA Today 25 Feb 2002) http://www.usatoday.com/life/cyber/tech/2002/02/26/cybersex.htm

Category 31.1 Surveys, studies, audits of security

2002-03-20 e-commerce wireless cellular mobile phone survey study e-payments

NewsScan; http://online.wsj.com/article/0,,SB1016559287588926040.djm,00.html (sub req'd)

# CONSUMERS WANT M-COMMERCE 'SIMPLE AND SMALL'

Consumer enthusiasm for mobile commerce -- buying goods and services via cell phones -- has dwindled since 2000, with only 1% of mobile users surveyed worldwide in January saying they intend to use Internet-enabled phones for any type of transaction. That's down from 12% a year earlier and 32% in June 2000. "The more they have used it, the less they have liked it," says a consultant at A.T. Kearney in London. However, 44% of the 5,600 wireless customers polled said they would be interested in finding out more about "m-cash" -- systems that allow users to make small purchases by dialing a number on the mobile phone and then having the charge included on the monthly phone bill. Companies already experimenting with m-cash include Pepsi, which has launched an m-cash program for distributors in the U.S. Cingular Wireless and Vodafone have also initiated limited m-cash services. Despite consumer interest, enthusiasm risks being derailed by the technical difficulty of installing the necessary hardware infrastructure to accommodate m-cash transactions. "It's convenient from a consumer perspective because it removes the need for small cash," says a marketing manager for Visa International. "But if you're going to retrofit every vending machine just to have people zap it with their mobile phones, I don't think there's a business case for that." Additional questions arise over the willingness of wireless carriers to act as the collector of other companies' debts.

"There's a substantial credit risk related to this," says a Scandinavian banking expert. (Wall Street Journal 20 Mar 2002)

Category 31.1 Surveys, studies, audits of security

2002-04-04 security threats vulnerabilities survey attitudes beliefs viruses hackers terrorists

Security Wire Digest, 4 26

http://www.instat.com/press.asp?ID=162&sku=IN020154NA

Security Wire Digest reported, "... [A] recent survey says infosec spending continues to be driven by the threat of hackers and viruses. According to InStat, a technology market research firm, ... 80 percent of the businesses it survey have the same attitude toward network security as they did prior to the Sept. 11 attacks and that they are more concerned about viruses and hackers than terrorists."

Category 31.1 Surveys, studies, audits of security

2002-04-08 computer crime survey statistics study

NewsScan:

http://news.bbc.co.uk/hi/english/sci/tech/newsid\_1916000/1916655.stm

#### COMPUTER CRIME WAY UP, SAYS FBI

Eighty-five percent of respondents report having been victims of computer crime, costing them millions of dollars, according to a survey by the Computer Security Institute and the FBI. The study, which polled 583 computer security experts in business, government agencies, medical institutions and universities, concluded that the most serious losses stemmed from theft of proprietary information. In addition, almost all of the organizations had suffered from computer virus attacks last year, and 90% said they had been victims of Web site defacement in 2001, up from 64% a year earlier. "Organizations that want to survive in the coming years need to develop a comprehensive approach to information security, embracing both the human and technical dimensions," says Patrice Rapalus, director of the Computer Security Institute. In response to the growing threat of cybercrime, the FBI has set up the National Infrastructure Protection Center and has formed regional Computer Intrusion Squads in several offices throughout the U.S. (BBC Online 8 Apr 2002)

Category 31.1 Surveys, studies, audits of security

2002-05-15 data overload productivity study research report signal-to-noise ratio social

interaction worklow tools utility saturation

NewsScan

#### DATA DYSPEPSIA

The quantity of information flowing into your office on a daily basis has reached an officially indigestible level, says Gartner, which reports that 90% of companies are suffering from data overload to the point where it's affecting their productivity. Gartner estimates that businesses will spend as much as \$30 billion this year alone on information management systems in the hope of digging out, but it still may not be enough to improve the signal to noise ratio in most offices. Surprisingly, Gartner found that the most useful information employees receive comes from personal contacts, contact with friends and colleagues and e-mails, rather than the corporate Intranet. The company has therefore recommended that businesses encourage more social interaction -- in cafeterias, lounges and around the water cooler -- while at the same time implementing workflow tools that can help stem the tide of useless information. (The Register 15 May 2002)

http://www.theregister.co.uk/content/23/25283.html

Category 31.1 Surveys, studies, audits of security

2002-05-30 software piracy stealing attitudes beliefs survey study ethics morality

NewsScan

#### IS STEALING WRONG ALWAYS, OFTEN, SOMETIMES, OR NEVER?

A new survey commissioned by the Business Software Alliance indicates that more than 50% of Americans who use the Internet regularly download commercial software without paying for it -- and that only 12% think that what they're doing should be considered piracy. Other depressing findings for software developers were that 43% of the survey respondents strongly agreed with the statement: "It makes no sense to charge me hundreds of dollars per user license vs. pennies to reproduce," and 22% somewhat agreed with: "The technology industry is so prosperous that a few people using unlicensed software won't make any difference." On the other hand, the modestly good news for developers is that 54% of respondents strongly agreed with the statement: "People that develop software deserve to be rewarded for their efforts." (San Jose Mercury-News 29 May 2002)

http://www.siliconvalley.com/mld/siliconvalley/3363169.htm

Surveys, studies, audits of security Category 31.1

2002-06-04 e-commerce Web design usability study survey

NewsScan; http://news.com.com/2100-1017-931274.html

#### E-COMMERCE SITE DESIGN IS \*SLOWLY\* IMPROVING

A new study by the Nielsen Norman Group that examined 15 e-commerce Web sites, including those of Martha Stewart, L.L. Bean and Office Depot, indicates that their usability quotient is increasing, but only slightly. A similar study conducted two years ago concluded that the sites met an average of 45% of the group's usability guidelines; that percentage is now 49%. "If we continue at this rate for the next 15 years, we will reach a level that we really want to be at," says Jakob Nielsen. "Fifteen years is a long time to wait to get good services on the Internet, but in the big picture, this is a new technology, and whenever anything else was invented, it took awhile to get it right." Among the sites studied this year, L.L. Bean came in on top, meeting 66% of the 207 usability guidelines. The guidelines cover everything from whether a site's product search engine can handle misspellings to whether a site requires a customer to select a state as part of their information profile -- something foreign visitors can't do. (CNet News.com 3 Jun 2002)

Category 31.1 Surveys, studies, audits of security

2002-06-06 survey financial costs QA quality assurance software testing research report

RISKS; http://www.nist.gov/director/prog-ofc/report02-3.pdf

22 11

NIST engaged the Research Triangle Institute (RTI) to assess the cost to the U.S. economy of inadequate software testing infrastructure. Inadequate testing is defined as failure to identify and remove software bugs in real time. Over half of software bugs are currently not found until downstream in the development process leading to significant economic costs. RTI identified a set of quality attributes and used them to construct metrics for estimating the cost of an inadequate testing infrastructure. Two in depth case studies were conducted. In the manufacturing sector, transportation equipment industries were analyzed. Data were collected from software developers (CAD/CAM/CAE and product data management vendors) and from users (primarily automotive and aerospace companies). In the service sector, financial services were analyzed with data collected again from software developers (routers and switches, financial electronic data interchange, and clearinghouse) and from users (banks and credit unions). .... [T]he annual cost to these two major industry groups from inadequate software infrastructure is estimated to be \$5.85 billion. Similarities across industries with respect to software development and use and, in particular, software testing labor costs allowed a projection of the cost to the entire U.S. economy. Using the per-employee impacts for the two case studies, an extrapolation to other manufacturing and service industries yields an approximate estimate of \$59.5 billion as the annual cost to the nation of inadequate software testing infrastructure.

Category 31.1 Surveys, studies, audits of security

2002-06-12 survey study online business e-commerce growth

NewsScan; http://online.wsj.com/article/0,,SB1023828339638741520.djm,00.html (sub req'd)

#### MAIL-ORDER/E-TAIL HYBRIDS LEAD E-COMMERCE INTO THE BLACK

Online retail sales rose 21% last year to \$51.3 billion and are expected to grow by 41% to \$72.1 billion this year, with mail-order catalogue companies racking up the most revenues. "What was remarkable to me is that the online portion of retail continued to grow, not at the same pace as in the past, but still solid improvement in a pretty dismal year," says Elaine Rubin, chairman of Shop.org, which commissioned the study by Boston Consulting Group and Forrester Research. The report predicts that the Internet retailing category as a whole will break even on an operating basis for the first time this year. Catalogue companies, like L.L. Bean and Lands' End, are leading the pack, showing a 6% operating margin last year, excluding interest and taxes. Meanwhile, bricks-and-mortar retailers showed a -5% operating margin last year, while Web-only companies had a -13% operating margin. Online retailing as a whole continues to represent only a sliver of total retail sales -- 2.4% last year and an anticipated 3.2% this year. However, in specific markets, such as computer hardware and software sales, e-tailing has made significant inroads, accounting for 17.9% of those sales last year, rising to a projected 23.4% this year. (Wall Street Journal 12 Jun 2002)

Category 31.1 Surveys, studies, audits of security

2002-06-14 music piracy intellectual property economic effects sales increase

NewsScan

#### MUSIC DOWNLOADERS MAY BE RECORD LABELS' BEST CUSTOMERS

Four out of five people who download music from the Internet report that their CD purchasing frequency either remained the same or increased, according to a new study by Ipsos Reid that concludes downloading music and burning CDs may actually stimulate legitimate sales. The research backs up an earlier study by Jupiter Media Metrix that concluded people using file-sharing networks were more likely to spend money on music. "While the goal of this was not to draw a link between file sharing, CD burners and the slump in music sales, we can see that American music enthusiasts are becoming increasingly acquainted with the flexibility that digital music allows," says a senior research manager at Ipsos Reid. "As a result, (American consumers) may be more apt to venture beyond the traditional channels of music distribution as part of their audio behaviors." (Wired.com 14 Jun 2002)

http://www.wired.com/news/mp3/0,1285,53157,00.html

Category 31.1 Surveys, studies, audits of security

2002-06-17 telecommuting confidentiality tunneling VPN encryption productivity

NewsScan

# TELECOMMUTING STILL GAINING IN POPULARITY

The number of U.S. workers toiling at home three or more days a week rose nearly 23%, from 3.4 million in 1990 to 4.2 million in 2000, according to U.S. Census figures. Meanwhile, the estimated number of workers who telecommute at least some portion of the week jumped more than 42% in two years, from 19.6 million in 1999 to 28 million in 2001, according to the International Telework Association and Council (ITAC). Most telecommuters live in New England and on the East and West coasts in areas with dense population and notorious traffic congestion, and more than two-thirds of telecommuters polled for an ITAC survey expressed satisfaction over their at-home worker status. "They're saying, 'This is three hours I don't need to be in the car, and I could be with my kids, pick (up) the dry cleaning, or whatever," says ITAC president Tim Kane. A formal E-Worker program instituted two years ago at Cigna Corp. has seen productivity increases of up to 15% among teleworkers while job turnover rates in some divisions of the company were cut in half. (AP 16 Jun 2002) http://apnews.excite.com/article/20020616/D7K6EEM00.html

Category 31.1 Surveys, studies, audits of security

2002-07-01 PC workstation personal computer sales broadband digital divide

NewsScan

#### PC SALES HIT THE 1 BILLION MARK

Approximately 1 billion PCs have been shipped worldwide since the mid-1970s, according to a new Gartner report, which predicts the next billion sales won't take nearly as long. Thanks to declining prices, the growth of the Internet, and the rapid adoption of computers in the developing world, the number of PCs shipped likely will double by 2007 or 2008. In addition, broadband proliferation is expected to boost shipments, with studies showing that broadband subscribers in the U.S. use their PCs more often and for more functions than do consumers with dialup accounts. "This demand exists because of the power of the PC to leverage intellectual capital, unlocking the capabilities of individuals to succeed and companies to profit," says the report. "However, expanding the market will require that PCs become smaller and even less expensive than they are today, while delivering greater functionality and performance," says the study. About 80% of the computers shipped to date have been desktop models, while notebooks have accounted for 16% of sales. (CNet News.com 30 Jun 2002) http://news.com.com/2100-1040-940713.html?tag=fd\_top

Category 31.1 Surveys, studies, audits of security

2002-07-05 search engine e-mail user utilization popularity

NewsScan

#### SEARCHING, NOT SURFING, IS NO. 1 NET ACTIVITY

Internet users increasingly are focusing their computer time on finding specific information via search engine, rather than aimlessly clicking from one site to the next, according to new statistics collected by the Pew Internet Project. More than 80% of all U.S. users have employed a search engine, and 29% of respondents turn to search engines every day to locate information online. Among Internet users who've been online for three years or more, the percentage of daily search engine users rises to 40%. The only activity more popular than searching is e-mail, which 52% said they did on a daily basis. The survey results indicate that people are learning to trust the results produced by search engines, and tend to rely on them rather than scouring the Web on their own. Google ranked No. 1 in popularity, based on the average number of minutes people spend using it per month. (BBC News 5 Jul 2002)

http://news.bbc.co.uk/hi/english/sci/tech/newsid\_209700

Category 31.1 Surveys, studies, audits of security

2002-07-08 criminal hackers crackers attacks report infowar information warfare Internet targets

NewsScan

# DOROTHY DENNING SAYS SURFCRACKERS FOLLOW THE MONEY

Renowned cybersecurity expert Dorothy Denning, a Georgetown University professor whose expertise includes information warfare, is not very surprised by a new report showing a 28% increase in the last six months in Internet attacks targeting technology, financial services and power companies: "In the hacker community, you are going to score more points for hitting bigger companies. There is also an economic gain to going after the large financial services targets — they have the money." The report, prepared by Alexandria, Va.-based security firm Riptech Inc., found more than 180,000 successful Internet attacks between January and June 2002. (Washington Post 7 Jul 2002)

http://www.washingtonpost.com/wp-dyn/articles/A36498-20

Category 31.1 Surveys, studies, audits of security

2002-08-01 information value cost consumer contracts Web economics e-commerce

NewsScan

#### INFORMATION WANTS TO BE PAID FOR

A new survey by the Online Publishers Association has found that in 2001 consumers spent nearly double in online purchases what they had spent the year earlier. Not surprisingly, people are most willing to pay money for business and financial information, because that kind of information influences their livelihood -- but beyond that there is a more general trend toward increased consumer willingness to pay for online content. One example: there are now more than a million subscribers to the online greeting card company American Greetings.com, which charges \$11.95 a year for virtual cards. Its chief executive says: "In the past five years, we trained customers that content was free -- that was our fault." And now? "Slowly but surely, people are paying for content." (New York Times 1 Aug 2002) http://www.nytimes.com/2002/08/01/technology/01ONLI.h

#### FOUR FLORIDA NEWSPAPERS TO CHARGE FOR WEB ACCESS

Four newspapers in the Florida Panhandle, all four owned by Freedom Communications, have decided to start charging for access to their Web sites. Freedom's chief executive says: "We felt there's value to the content and we should get something for the value of the content." The editor of one of the papers adds: "People who work expect to get paid, whether they deliver information or they deliver pizzas." The newspapers have received a barrage of complaints from their readers for the move they've taken. (AP/New York Times 4 Aug 2002)

Category 31.1 Surveys, studies, audits of security

2002-08-14 intellectual property music sales piracy study

NewsScan

#### BLAME THE ECONOMY, NOT PIRACY, FOR WEAK CD SALES

A Forrester Research report released Tuesday [Aug 13] says that the true threat to record labels' profits is the sagging economy, and that downloadable music could actually prove to be the industry's salvation rather than its scourge. According to the report's findings, people who download music from the Internet more than nine times a month — a relatively small percentage of the overall market — say they'll decrease their album purchases by 2%. At the same time, 39% of downloading enthusiasts said they bought more CDs, because they found new music that they wanted to purchase through their file-swapping activities. Meanwhile, it turns out that consumers who rarely or never download music account for more than two-thirds of CD sales in the U.S. With music sales slumping nearly 10% this year so far, report author Josh Bernoff says the true culprits are limited radio playlists, high-priced CDs and a general economic recession. The Forrester report suggests that record labels should offer more flexible pricing and online access to their entire music back-catalogues in order to make online music-buying more consumer-friendly. The predicted payoff (which some view as excessively optimistic) could amount to a boost of \$937 million in album downloads, \$805 million in singles downloads and \$313 million in subscription fees by 2007. (Los Angeles Times 14 Aug 2002)

Category 31.1 Surveys, studies, audits of security

2002-08-20 information warfare infowar homeland defense backup antivirus survey

NewsScan

# SMALL BUSINESSES SHORE UP THEIR CYBERSECURITY DEFENSES

A Computer Economics survey of 233 U.S. corporations by has found that since September 11 about 77% of businesses have improved their defenses against network vandals, viruses and other cyberattacks. Although smaller firms typically have the most reluctance to hire full-time security professionals, Computer Economics says that companies with less than \$1 million in annual revenue represent the biggest proportion of companies that have improved their security with anti-virus programs and backup equipment during the past year. (USA Today 19 Aug 2002)

Category 31.1 Surveys, studies, audits of security

2002-08-27 intellectual property music sales piracy study

NewsScan

#### LABELS CLAIM DOWNLOADING CUTS INTO CD SALES

In contrast with the findings of a recent Forrester Research study [see entry for 2002-08-14], the Recording Industry Association of America has unveiled its own study that claims Internet users who say they are downloading more music are also buying fewer CDs. "Among people who said their downloading from file-sharing services had increased over the past six months, 41% reported purchasing less music now than six months ago, compared to only 19% who said they were purchasing more music," the RIAA said in a statement. Jonathan Potter, executive director of the Digital Media Association, downplayed the utility of studies such as the RIAA's. "The way to defeat illegal music distribution services is to offer comprehensive, innovative, fairly priced legal services. Until the record companies offer their content ubiquitously in a consumer-friendly way, studies like this are useless." In response to record labels' complaints that it's unfair to expect them to compete successfully in selling a music subscription service when fans can get the same songs for free, Potter says, "I'd like to introduce the recording industry to something called bottled water? The point is if there were a high-quality product that was affordable and available across multiple services, they would be able to defeat the free services." (Reuters/CNet 26 Aug 2002) http://news.com.com/2100-1023-955397.html?tag=fd\_top

Category 31.1 Surveys, studies, audits of security

2002-08-28 online sales survey study growth e-commerce

NewsScan

#### ONLINE RETAIL SOARS 24%

Online retail sales jumped 24% in the second quarter in year-over-year results from the same period in 2001, according to a report from the U.S. Census Bureau that defies the conventional view of e-commerce as a struggling sector. In fact, while online retail grew 24%, total retail grew by only 2.5%, year-over-year. Leading the numbers, which did not include sales from online travel, finance and ticketing sites, were books and apparel. Aggressive moves by Amazon and Barnes & Nobles to offer free shipping have boosted online book sales and J.Crew recently reported that it continued to take in more revenue through its Web site than it did over the phone -- a milestone reached last February. "It wasn't a blip," says a Jupiter Media Metrix analyst Ken Cassar. And what's ahead? With the threat of recession looming, third quarter sales are expected to taper off a bit, but the fourth quarter -- traditionally the strongest -- is expected to be huge. According to Jupiter, the percentage of consumers' holiday purchases bought online is growing every year. (Business 2.0 26 Aug 2002)

Category 31.1 Surveys, studies, audits of security

2002-09-06 Internet Web monitoring surveillance content filntering e-mail

NewsScan

#### ATTITUDES ABOUT RESTRICTIONS OF INFORMATION ON THE WEB

An opinion survey conducted by the Pew Internet and American Life Project found that two-thirds of Americans think it's appropriate for government agencies to exclude some information from their Internet postings, and about half think it's all right for government to monitor Web and e-mail activities. David Greene of the First Amendment Project in Oakland, California, worries: "It certainly is significant that our society which has always prided itself on open access of information is now so scared of what open access to information means. People think, 'I'm not going to poison the water system, so what do I need to know about the water supply system?' But if all of a sudden they are part of an effort to restrict development of a watershed and need that data ... all of a sudden it's important." (AP/San Jose Mercury News 5 Sep 2002)

Category 31.1 Surveys, studies, audits of security

2002-10-01 Internet sociology culture effects influence democracy culture digital divide

research clearinghouse center projects

NewsScan

#### NEW INSTITUTE EXAMINES INTERNET'S IMPACT

The Oxford Internet Institute opened its doors last week — one of the world's first research centers dedicated to studying the Internet and its social consequences. The Institute is structured as a multidisciplinary organization that will house its own teaching staff, carry out its own research, and act as a collection point and clearinghouse for Internet research projects. Institute director Bill Dutton notes that the Internet is already profoundly changing many social relationships: "The fundamental implication of changes in information technology is that it reconfigures access. Not just in terms of the digital divide but also who you know, what you know and what you get access to and use." Meanwhile, Eli Noam, professor of economics and finance at Columbia University, warns against simply assuming that the Net is a force for good all by itself and needs no outside guidance. He notes that rather than flattening social structures and breaking down barriers, today's Internet is concentrating information in the hands of smaller groups. "We need academics to be leaders, not cheerleaders. We must save the Internet from its founding myth that it is good for democracy and is open and cannot be regulated." (BBC News 1 Oct 2002)

http://news.bbc.co.uk/1/hi/technology/2288598.stm

Category 31.1 Surveys, studies, audits of security

2002-11-03 online music sales copyright intellectual property piracy survey study

NewsScan

#### ONLINE MUSIC SALES PLUMMET

Statistics from ComScore Media Metrix show that online sales of new music fell 20% in the first half of the year, and 39% for the third quarter. This happened during a period in which online sales for most other categories (such as computer hardware, office equipment and supplies, apparel, consumer electronics, and books) increased over last year's figures. ComScore president Peter Daboll says, "People are buying less and burning more. I'd be worried if I was selling music." (USA Today 3 Nov 2002)

Category 31.1 Surveys, studies, audits of security

2002-11-22 Internet usage digital divide study survey growth e-commerce international

NewsScan

#### GLOBAL NET USE CONTINUES TO BOOM

Despite the current economic gloom and the sharp contraction of the technology industry over the past couple of years, global use of the Internet continues to soar and e-commerce is expanding at a robust pace, according to this year's "E-Commerce and Development Report" issued Monday by the U.N. Conference on Trade and Development. The annual study predicts that the value of goods and services sold over the Net could reach as high as \$2.3 billion this year, a 50% rise from last year, and could go as high as \$3.9 billion by the end of 2003. Meanwhile, m-commerce is forecast to generate revenues of almost \$50 billion in 2002, with Western Europe and North America leading that market for the next three years. The report cites SMS, or text messaging, as the dominant driver of m-commerce revenues, followed by micro-payments, financial services, logistics, information services and wireless customer relationship management. However, concerns over security and difficulties in making electronic payments are "limiting the conduct of m-commerce," warns the report. (PCWorld.com 21 Nov 2002) http://www.pcworld.com/news/article/0,aid,107219,00.asp

Category 31.1 Surveys, studies, audits of security

2002-12-09 e-mail deluge overload survey study myth

NewsScan

### SURVEY DEBUNKS MYTH OF THE E-MAIL DELUGE

The latest study from the Pew Internet and American Life Project indicates that reports of massive e-mail volume swamping workers and sapping their productivity are greatly exaggerated: in fact, 60% of Americans who use e-mail at work receive 10 or fewer messages on the average day, and three-quarters reported spending an hour or less daily dealing with e-mail. Only 6% reported receiving more than 50 e-mails a day, and among those, only 11% said the volume posed a problem. Most workers who receive a lot of e-mail have devised ways to manage the load, such as using filters to automatically sort the mail into folders. "All of the anecdotal evidence you hear from people out there is, 'I'm so overwhelmed by the volume of e-mail. The perception comes from the people who are talking most loudly about it, those few who are most overwhelmed," says Pew senior research fellow Deborah Fallows. The pattern is different for power users, typically those in high-level managerial positions at large corporations. Many of them spend at least two hours daily on e-mail, with the task often stretching out to four or more hours. Meanwhile, the study found that younger users (those under 30) are more likely to use e-mail for personal use while at work, often sending gossip, jokes and chain letters while on the job. (AP 8 Dec 2002) http://apnews.excite.com/article/20021208/D7NPSN680.htm

Category 31.1 Surveys, studies, audits of security

2002-12-11 broadband Internet access cable International trends study

NewsScan

#### DSL GROWTH SURGES TO RECORD HIGH

The number of consumers signing up for DSL (digital subscriber line) service increased nearly 20% between July 1 and September 30 over the previous three-month period -- an unprecedented growth rate, according to a DSL Forum survey. Findings indicate there are now about 30 million DSL users globally, although in the U.S. cable modem users still outnumber DSL subscribers about 2 to 1. "In the U.S., (cable modem providers) are beating the hell out of us," says DSL Forum chairman William V. Rodey. "But globally, we're beating the hell out of them." Outside the U.S. there are only about 5 million cable modem customers, while foreign DSL subscribers number about 22.5 million. Tops in DSL subscriber numbers is the Asia-Pacific region (with South Korea ranking highest), followed by Europe (thanks to strong growth in Germany, Norway and Croatia), with the U.S. coming in third. (CNet News.com 10 Dec 2002) http://news.com.com/2100-1033-976791.html

# 31.2 Estimates, guesses, predictions, forecasts concerning security

Category 31.2 Estimates, guesses, predictions, forecasts concerning security

2002-01-04 criminal hacker targets home PC wireless networking firewalls antivirus education

awareness vulnerability warnings predictions

#### NewsScan

#### HOME PCs -- THE NEXT HACKER TARGET

Computer hackers are turning their sights to the humble home PC, which is now faster, more powerful and less secure than ever before. Fueling the onslaught are several factors, including the trend toward home-based DSL or cable connections that are "on" all the time, and the lackadaisical attitudes of most home PC owners who generally don't keep up to date with the latest antivirus and firewall software. In addition, many home users are naïve about the potential threat and willingly click on unsolicited e-mails that could be infected with malicious programs. "Home users have generally been the least prepared to defend against attacks," warns Carnegie Mellon's Computer Emergency Response Team Coordination Center. "In many cases, these machines are then used by intruders to launch attacks against other organizations." Antivirus firm Message Labs reported that it detected one virus per 370 e-mail messages in 2001, double the rate of the previous year. Meanwhile, Amit Yoran of computer security firm Riptech says the advent of wireless networking will increase the risk of attack significantly: "The standard itself is insecure What we're faced with is the widespread adoption [of wireless networks] throughout corporate America and throughout consumer markets and people haven't really thought through how to protect." (AP/Wall Street Journal 4 Jan 2002)

http://interactive.wsj.com/articles/SB1010104082304162760.htm (sub req'd)

Category 31.2 Estimates, guesses, predictions, forecasts concerning security

2002-01-10 copyright intellectual property music sales prediction analysis royalties fees

#### NewsScan

2002: THE YEAR OF THE COPYRIGHT? "The recording industry has vowed to make 2002 the year of the copyright," says columnist Patti Waldmeir. To further that goal, record labels are experimenting with CDs that include technology that prevents them from being copied, even by owners for their own use, and several online music subscription services set to launch this year will be engineered to prevent unauthorized reproduction. If the technology is successful, it could be the year of ascendancy for copyright holders, who will find themselves wielding more power than was ever intended under U.S. copyright law or the constitution, says Stanford University law professor Lawrence Lessig. Lessig argues that by extending the term of copyrights 11 times in the last 40 years, Congress has exceeded its constitutional authority, granting copyright holders terms that extend long beyond a human lifetime. Lessig argues that these over-lengthy terms violate the constitution's command to "promote the Progress of Science and the useful Arts, by securing for limited Times to Authors and Inventors the exclusive Right to their respective Writings and Discoveries." Under today's technology, the copyright on a locked CD may expire, but the CD would remain locked. In Lessig's recent book, "The Future of Ideas: The Fate of the Commons in a Connected World," he recommends a radical revision of copyright law: copyright protection should be cut to five years, renewable 15 times. If a copyright is not renewed, the work would enter the public domain. (Financial Times 10 Jan 2002) http://news.ft.com/news/industries/media

Category 31.2 Estimates, guesses, predictions, forecasts concerning security

2002-01-11 copy protection music piracy countermeasures prediction public rejection resistance

# NewsScan

#### PHILIPS SAYS COPY-PROTECTED CDs WON'T LAST LONG

Philips Electronics, which invented the compact disc, says the controversial attempts by the recording industry to market "copy protected" CDs will fail because consumers just don't like it. As inventor of the CD standard and the industry's licensing body, Philips says it could refuse to license the new discs as genuine CDs or pursue some kind of legal action, but thinks the copy-protected CDs will disappear on their own as consumers reject them. "Any kind of legal action would take years and we don't expect these [discs] to last that long," says Gary Wirtz, general manager of the Philips Copyright Office. "At the moment we are trying to reason with people rather than sue them. [The technology is] not going to work, because any hacker can still make copies. It's only going to affect legitimate consumers and we know there have already been considerable complaints." Philips opposes the technology because it can make legitimate CDs unplayable in some older players and in-car audio systems. Critics maintain that the technique used to block copying can also impair the quality of a disc's audio content over time. (New Scientist 11 Jan 2002)

http://www.newscientist.com/news/news.jsp?id=ns99991783

Category 31.2 Estimates, guesses, predictions, forecasts concerning security

2002-02-06 survey study statistics prediction security budgets spending industry

NewsScan

#### CORPORATE SPENDING ON INFORMATION TECHNOLOGY

A Goldman Sachs survey of information technology executives at 100 large corporations suggests that tech spending will be flat in the year ahead. The only areas that would see increases are expected to be security software, data networking, database software, storage software, and disaster recovery. (Reuters/San Jose Mercury News 6 Feb 2002) http://www.siliconvalley.com/docs/news/svfront/057894.htm

Category 31.2 Estimates, guesses, predictions, forecasts concerning security

2002-06-17 online medicine e-commerce privacy confidentiality

NewsScan

#### DOCTORS TO MAKE VIRTUAL 'HOUSE CALLS'

Medem Inc., the for-profit Internet company backed by the American Medical Association and other physician groups, is launching a new service that will enable doctors to offer online consultations to established patients for a fee. The Medem service allows patients to pay upfront with a credit card, which alleviates one of most doctors' biggest concerns -- problems with payment. However, most patients will be footing the bill for online consultations themselves -- outside of a few trial programs, e-mail consultations aren't reimbursed. Physicians interviewed suggested they'd probably charge \$20 to \$30 a virtual visit. (Wall Street Journal 17 Jun 2002)

http://online.wsj.com/article/0,,SB1024265768750036320.djm,00.html (sub req'd)

Category 31.2 Estimates, guesses, predictions, forecasts concerning security

2002-06-19 hacktivism Web vandalism penetration hacker attack information warfare

NewsScan;

http://news.bbc.co.uk/hi/english/sci/tech/newsid\_2052000/2052320.stm

#### PRO-ISLAMIC GROUPS ENGAGE IN 'HACKTIVISM'

UK security firm mi2g says there's mounting evidence that individual hacker groups with a pro-Islamic agenda are working together to disrupt Web sites in India, Israel and other target countries. "Political motivation is an increasingly rising factor in digital attacks," says mi2g CEO DK Matai. "The primary reason why Web attacks are increasing is political tensions between Israel and Palestine, India and Pakistan, and China and Taiwan." Israel has suffered a barrage of attacks since the beginning of the latest Palestinian uprising in September 2000, and during the recent tensions between India and Pakistan over Kashmir, several groups (including Unix Security Guards, Anti-India Crew and World Fantabulous Defacers) have carried out hundreds of attacks on Indian educational and business Web sites. Despite the increase in attacks, the total number of new viruses has actually been decreasing, says mi2g, following a peak in 1997. However, each new virus is capable of causing more trouble because of the large number of computers that are now networked together. "When one catches a cold the entire global organization catches it," says Matai. (BBC News 19 Jun 2002)

Category 31.2 Estimates, guesses, predictions, forecasts concerning security

2002-06-19 covert channels wireless communications tooth biological interface

NewsScan

### 'TOOTH PHONE'

Engineers in the UK say they've developed a tooth implant that incorporates a tiny vibrator and a radio wave receiver, and is capable of functioning like a tooth-based cell phone. The implant does not yet have its own microchip installed, but inventors James Auger and Jimmy Loizeau say the technology has been tested, and that a fully functional phone is feasible. Sound, received as a digital radio signal, would be transferred to the inner ear by bone resonance, enabling information to be received anywhere and at any time, with no one else the wiser. The invention raises the possibility of financial traders receiving the latest stock market updates while taking in a movie, or politicians receiving a secret briefing on the issues while being quizzed by reporters. (Reuters 18 Jun 2002)

http://news.com.com/2100-1033-937253.html

Category 31.2 Estimates, guesses, predictions, forecasts concerning security

2002-06-21 wireless Internet service in-flight

NewsScan

#### IN-FLIGHT INTERNET GETS ANOTHER BOOST

Boeing's efforts to bring in-flight high-speed Internet access to airline passengers received a major boost when it announced British Airways as its second trial customer. Up until now, Lufthansa has been the only other airline signed on for Connexion's pilot project. Boeing is struggling to keep the project on track following the decision of three U.S. airlines -- American, United and Delta -- to back out of plans to take an equity stake in the venture following last September's terrorist attacks. British Air marketing director Martin George says he's confident the trial will be a success: "What our customers are saying to us is we would like the option (of broadband access) onboard. This is the future of in-flight entertainment. I would like this in the cabin of all our long-haul aircraft as soon as possible." The Connexion system eventually will supply live TV and can also be used to transmit data about the aircraft back to the ground. (Financial Times 13 Jun 2002)

http://news.ft.com/servlet/ContentServer?pagename = FT.com/StoryFT/FullStory&c = StoryFT&cid = 1023858976044&p = 1012571727248

#### MITSUBISHI, BOEING TEAM UP ON IN-FLIGHT INTERNET SERVICE

The Mitsubishi Electric Corporation will manufacture antennas for an in-flight Internet service that Boeing Aircraft will offer as "Connexion by Boeing," with tests of the service beginning in next January [2003]. Boeing's announcement was enthusiastic, with an executive proclaiming that the service is "about choice. It's about tomorrow. It's about a good partnership we're excited about. We can't imagine a better partner." (AP/San Jose Mercury-News 21 Jun 2002) http://www.siliconvalley.com/mld/siliconvalley/3516860.htm

Category 31.2 Estimates, guesses, predictions, forecasts concerning security

2002-07-02 click-through e-mail ads spam study survey estimate

NewsScan

#### ONLINE ADS FAIL TO CLICK WITH VIEWERS

Consumers are tired of online ads, according to a recent study by eMarketer, which estimates that the average click-through rate on e-mail ads is a paltry 1.8%. That's down from 3% last year, and reflects what eMarketer senior analyst David Hallerman calls a radical shift in consumer psychology: people are so overwhelmed with the daily avalanche of e-mail advertisements, that they just aren't as curious about what they're selling as they used to be. The findings are consistent with recent estimates from DoubleClick, which pegged the average click-through rate for all online ads in June at 0.84%. During the heyday of online advertising, companies could expect a click-through rate as high as 15% for some promotions. Unfortunately, the technology's success is what's leading to its demise -- companies will blast consumers with more than 430 billion e-mail ads this year; by 2006 it's expected to rise to more than 960 billion. "The same thing happened to paper-based direct mail when it first became popular in the early 1980s," says a Forrester analyst. "By the mid-1980s, scores of companies were doing it, and everyone's mailboxes were jammed so they began standing over their trash baskets making the quick decision. Today, they are opening their e-mail boxes and often they are just hitting the delete key." (Wall Street Journal 2 Jul 2002) http://online.wsj.com/article/0,SB1025554487479274320.... (sub req'd)

Category 31.2 Estimates, guesses, predictions, forecasts concerning security

2002-07-30 broadband network ISP Internet service providers growth prediction

NewsScan

### BROADBAND: GROWING BUT SLOWING

The research firm In-Stat/MDR predicts is predicting that the number of broadband subscribers worldwide will increase by 50% this year, reaching about 46 million). That's quite a change from the period 1999 to 2001, when the growth rate exceeded 100% annually. The company also says that in the U.S. there were 7.12 million cable modern subscribers at the beginning of 2002, compared with 4.6 million subscribers for DSL; and it predicts that DSL will take the lead in the U.S. market by 2004. (New York Times 30 Jul 2002)

http://www.nytimes.com/pages/technology/index.html

Category 31.2 Estimates, guesses, predictions, forecasts concerning security

2002-08-07 e-commerce online sales

NewsScan

#### AUTO INDUSTRY RETHINKS ITS INVOLVEMENT WITH E-COMMERCE

Just three years ago, automakers GM, Ford, and DaimlerChrysler seemed frantic to get on the e-commerce train before it left the station. All of them committed millions of dollars to online sales efforts and created whole new divisions to support those efforts. But now it's quiet time, and automakers are resisting new online ventures until they feel completely sure that those ventures will generate profit. So the current situations is quite a contrast from the old, old e-commerce days (1999 or so). Karen Francis, Ford's former e-commerce chief, explains what it was like then: "You didn't know what you didn't know. You had to get in. You had to place a bet because the initial hype was such that this was going to provide unprecedented, fill in the blank, and no company wanted to be caught with their competitors having an unprecedented advantage." But that was then, this is now: time for taking a rest and closing the eyes. (AP/USA Today 6 Aug 2002)

Category 31.2 Estimates, guesses, predictions, forecasts concerning security

2002-08-14 Linux growth operating system prediction

NewsScan

#### MCNEALY PREDICTS 30% ANNUAL GROWTH IN LINUX USERS

Addressing participants at the Linux World Conference and Expo, Sun Microsystems CEO Scott McNealy predicted Tuesday that the number of Linux users will grow by 30% a year for the next several years, and urged companies to embrace the open-source software movement. Documenting his own company's commitment, McNealy noted that Sun has at least 400 full-time employees dedicated to Linux and pledged to abide by the ethical standards of the Linux community, which is made up of thousands of grassroots enthusiasts worldwide who collaborate on software projects. "We're going to share in the lifestyle and be a capitalist," said McNealy. "We'll share our thoughts but we don't think it's broken so we're not going to try to fix it," he said, referring to fears that companies could take the open source code and factionalize it by creating competing proprietary versions. (AP 13 Aug 2002)

http://apnews.excite.com/article/20020813/D7LCONLO1.htm

Category 31.2 Estimates, guesses, predictions, forecasts concerning security

2002-08-15 wireless telephones cellular mobile study predictions

NewsScan

#### THE UNFIXED LIFE

Some stats on telephone use: the FCC says there were 122.4 million wireless subscribers nationwide at the end of 2001, and industry analyst Keith Mallinson predicts that number will grow to 200 million by 2006. That's about 70% of the total U.S. population. Mallinson also expects that the number of people who rely completely on a wireless phone will rise from the current 3% of the population to somewhere between 5% and 10% in the next five years. (San Jose Mercury News 15 Aug 2002)

Category 31.2 Estimates, guesses, predictions, forecasts concerning security

2002-08-28 online banking e-commerce study survey analysis

NewsScan

#### ONLINE BANKING SLOW TO GO

A report from the Federal Reserve Bank of New York says that the acceptance of online bill-paying has been "very slow, falling far short of initial projections," because of a chicken-or-egg dilemma in which billers are reluctant to adopt electronic payment systems until they're confident they can sharply reduce their traditional paper-based systems, and customers are reluctant to put themselves in a situation in which they have to maintain both electronic and traditional methods of paying their bills. It has been estimated that the total cost of processing an individual check can range between \$1 and \$5, compared to less than one dollar for a fully electronic payment. (Dow Jones/AP/San Jose Mercury News 28 Aug 2002)

Category 31.2 Estimates, guesses, predictions, forecasts concerning security

2002-08-29 infowar information warfare attacks penetrations criminal hackers homeland defense infrastructure prediction survey

NewsScan

#### THE CHANCES OF FUTURE CYBERATTACKS

A survey of chief security officers taken by the new CSO Magazine found that 49% of 1,009 survey respondents believe that terrorists will launch a major strike through computer networks within the next 12 months. President Bush's Critical Infrastructure Protection Center shares that concern; CIPC official Tiffany Olsen says that all citizens have to do their share: "The average American doesn't necessarily recognize that he or she has a responsibility to protect their bit of cyberspace by using anti-virus software, firewalls, etcetera." (Reuters/San Jose Mercury News 29 Aug 2002)

Category 31.2 Estimates, guesses, predictions, forecasts concerning security

2002-09-17 wireless communications phones growth market

NewsScan

#### WIRELESS USE TO DOUBLE IN THE U.S. BY 2006

The number of monthly minutes of wireless use in the U.S. is expected to nearly double by 2006 from 2001 levels, according to a study by the Yankee Group. "Although only 3% of U.S. consumers use their mobiles as their only phone? 26% of mobile users' minutes are already being displaced from wireline to wireless and 45% of mobile users indicated at least some substitution," says the research firm, citing survey results. Analyst Keith Mallinson says he sees a strong demand for wireless services in the future, with the number of subscribers increasing to nearly 200 million by 2006 as 70% of Americans become mobile phone users, up from nearly 50% today. However, the industry's current stagnation could derail these predictions, Mallinson warns: "Buoyant market demand for mobile services? is in danger of being wrecked by a stalemate on the supply side. Limited scope for differentiation in the national marketplace has resulted in a price war, with too much capital and too many competitors resulting in anemic financial performance." (Reuters 16 Sep 2002) http://makeashorterlink.com/?Z271222D1

Category 31.2 Estimates, guesses, predictions, forecasts concerning security

2002-09-23 Web economic model payment fee for service value prices

NewsScan;

http://partners.nytimes.com/2002/04/22/technology/ebusiness/22ECOM.html

# INFORMATION WANTS TO BE PAID FOR

Pornography and gambling sites have profited from selling Internet "content" for years now, but the newest trend is for general information and service providers to "slice and dice" their offerings and give some away and charge for the rest. Forrester Research analyst Lisa Allen argues that content-providers need to "start acting less like a media company and more like a retailer," by testing and marketing different products at different prices for different segments of the customer population. Following examples set by the online operations of The Wall Street Journal and by Consumer Reports, the personal finance magazine Smart Money recently began to explore the idea of selling some of its online content. The general manager of SmartMoney.com predicts: "It's a matter of acceptance, and the more that companies to this, the more users will realize good content should be paid for."

# DOES REAL ESTATE INFO WANT TO BE FREE?

In its convention this fall, the National Association of Realtors (the country's No. 1 real estate trade association) will be considering a new rule that will let brokers withhold property information from Internet sites that give access to multiple listing services. Proponents of the rule say that such data is valuable information and that it belongs to the brokers who assemble and manage, while opponents say that brokers should see themselves as deal managers rather than as information gate-keepers. NAR general counsel Laurie Janik says that a multiple listing service "is a broker-to-broker tool. It's never been open to the consumer." (USA Today 22 Sep 2002)

http://www.usatoday.com/tech/news/realty2.htm

Category 31.2 Estimates, guesses, predictions, forecasts concerning security

2002-09-27 prognostications guesses predictions error gurus experts

NewsScan

#### HITS & MISSES IN HIGH-TECH PROGNOSTICATIONS

MIT Media Lab founder Nicholas Negroponte admits that he's missed the mark a few times in his predictions about the future of the high-tech industry, but he's got plenty of company -- Novell CTO Alan Nugent and Negroponte both thought people would be conversing with their computers years ago. Nugent also predicted that computers would be able to emulate human thought, but so far the only example of that ability is IBM's chess-playing computer, which still falls short of Nugent's expectations. Accenture chief scientist Glover Ferguson said his worst prediction was that the future of programming would focus on computer-aided software, and Concept Labs director Peter Cochrane said he mistakenly thought that voice-over-IP technology would be a dud. Michael Earl, dean of Oxford University's Templeton College said he greatly overestimated the ability of e-commerce to become a mainstream profit center, but that he's ready to predict that the future focus of the Internet will be much more on information than transactions. Meanwhile, Negroponte and Cochrane are betting that there will be a grassroots movement to supplant some of the services now offered by traditional telecom companies. The growth of Wi-Fi networks in the U.S. and the movement in Europe by local municipalities and universities to build and operate their own telecom networks will change the way telecom services operate forever, says Negroponte. "Telecom could invert itself and become a bottom-up phenomenon." (Wall Street Journal 27 Sep 2002)

Category 31.2 Estimates, guesses, predictions, forecasts concerning security

2002-09-30 spam e-mail volume denial of service DoS prediction content filtering overload

NewsScan

#### PREDICTION: E-MAIL WILL BECOME DOUBLE-TROUBLE IN 3 YEARS

IDC, the technology research firm, is predicting that within just three years, the number of e-mail messages sent worldwide will increase from the current level of 31 billion daily to more than 60 billion daily. Most of it will be spam (unsolicited commercial messages), and if the problem of spam is not dealt with by more effective message-filtering, the usefulness of e-mail as an effective business and personal communications tool will be endangered. IDC executive Mark Levitt says, "Like water flowing out of a hose, e-mail has the potential to fill our inboxes and workdays, overwhelming our abilities to navigate through the growing currents of content." (VNUNet 30 Sep 2002)

http://www.vnunet.com/News/1135485

Category 31.2 Estimates, guesses, predictions, forecasts concerning security

2002-10-03 robotics study predictions market growth

NewsScan

#### U.N. REPORT PREDICTS BIG JUMP IN ROBOT USE

The World 2002 Robotics Report, compiled by the U.N. Economic Commission for Europe, predicts that sales of all kinds of robotic devices for domestic use, excluding toys and games, will jump from 21,500 in 2001 to more than 700,000 during the 2002-2005 period. "Prices are going to come down just as they did for personal computers. When PCs started to be used by private people, they were pretty expensive," says Jan Karlsson, a UNECE expert who worked on the report. Sales of robots for all uses fell sharply last year, primarily as a result of plummeting demand in Japan and a depressed U.S. economy. But over the long haul, sales will soar and could even help alleviate a predicted worker shortage due to aging populations. The report forecasts a 50% jump in robot use in Europe by 2005, and a 30% rise in North America over the same period. (Reuters 3 Oct 2002)

http://makeashorterlink.com/?O1A161EF1

Category 31.2 Estimates, guesses, predictions, forecasts concerning security

2002-10-08 copyright intellectual property music software piracy Internet broadband bandwidth

speed

NewsScan

# BROADBAND THREATENS ASIAN ANTIPIRACY EFFORTS

Broadband technology is undermining efforts by software and entertainment companies to combat copyright piracy in Asia, say industry executives. "As broadband becomes more accessible and home PCs become more pervasive, the Internet is evolving as a whole new canvas for piracy," says Sanjay Mirchandani, Southeast Asia president for Microsoft. According to IDC Asia Pacific, 19% of South Koreans and 11.5% of Hong Kong residents have access to broadband, and these countries are among the worst offenders, says Harry Hui, Southeast Asia president for Universal Music. "Countries with broadband see the most downloads" of music from illegal Web sites, says Hui. Compounding the problem are the burgeoning number of illegal optical-disc factories in countries such as China, Malaysia and Indonesia. According to the Business Software Alliance, 50% of all business software used in Asia is copied or counterfeit, with China, Vietnam and Indonesia some of the worst offenders. (Wall Street Journal 8 Oct 2002)

Category 31.2 Estimates, guesses, predictions, forecasts concerning security

2002-10-16 terminology data volume Greek prefixes

NewsScan

#### STORAGE INDUSTRY MAXING OUT ON GREEK SUPERLATIVES

Having made short work of "mega" ("megas" is Greek for great), "giga" (giant) and "tera" (monster), the computer storage industry is scrounging around for new prefixes to describe the ever-increasing numbers of bytes it manages. In the near term, companies will be dealing with petabytes (from Greek "penta") and exabytes ("hexa"), but rapidly growing e-mail volumes and the increased value of e-mail will demand novel solutions. "We are already dealing with petabytes of data with video clips, and new services such as instant messaging will serve only to push demand further," says Veritas CTO Greg Valdez. "Companies must have a strategy for managing all of this data. If you don't have a strategy you are just going to keep adding more and more storage on the back of the e-mail servers." Valdez says future storage management software will be "smarter": "You need a smart file system to make it easier to access archives. Traditional file systems operate only at the block level and this is no longer enough. You must be able to manage it right down to the transaction level." Meanwhile, some software suppliers, like KVS, use data compression techniques to keep data volumes down. At least so far, no one's yet talking about "hepta" and "octa" bytes. (Financial Times 16 Oct 2002)

http://makeashorterlink.com/?D5DF21622

Category 31.2 Estimates, guesses, predictions, forecasts concerning security

2002-11-14 cyberterrorism attacks exaggeration infowar information warfare homeland defense

study analysis surveys

NewsScan

#### CYBERTERRORISM THREAT OVERHYPED, SAYS REPORT

A new report by the British firm mi2g says despite the scare-mongering tactics of government officials warning against "cyberterrorist" attacks, actual numbers of such attacks on government networks are declining worldwide. In the U.S., reported intrusions into government networks fell from 386 in 2001 to 162 in the first 10 months of 2002. Worldwide, such attacks have declined by a third -- from 2,031 last year to a projected 1,400 in 2002. The report was issued just a day after the U.S. Congress approved a \$903 million bill for beefing up government computer security and the Justice Department indicted a British cracker for breaking into military and NASA computer systems. Meanwhile, the overall number of computer attacks has doubled, from 31,322 in 2001 to 64,408 this year -- a trend that doesn't surprise Lawrence Walsh, editor of Information Security magazine: "Most of the attacks today are made by unsophisticated 'script kiddies' using off-the-shelf tools. What's the incentive for them to go after government systems? There are more rewards available from attacking small and medium-sized businesses -- like credit card information and financial data. And these networks are typically not as well-defended." (Wired.com 14 Nov 2002)

http://www.wired.com/news/politics/0,1283,56382,00.html

Category 31.2 Estimates, guesses, predictions, forecasts concerning security

2002-12-10 Wi-Fi wireless ISP Internet service provider study analysis

NewsScan

#### WI-FI: THE FUTURE ISN'T HERE YET

Wireless communications analyst Dylan Brooks of Jupiter Research says the industry is in "a bit of a bubble... We've had more than \$2 billion in venture capital money flowing in, more than total revenues." (Sounds like the Internet of yesteryear, doesn't it.) Everyone seems to agree that Wi-Fi is the future -- but the future won't be here for at least another few years. Synergy Research predicts that the industry's revenues won't top \$3 billion (1% the worldwide telecom equipment market) before 2003, and WiFi has yet to crack into the corporate market -- which is where the money is. Giga Information Group analyst Stan Schatt explains, "Most corporations are holding back because the suppliers cannot provide good security or tools for closely monitoring how the networks are performing." (New York Times 9 Dec 2002)

Category 31.2 Estimates, guesses, predictions, forecasts concerning security

2002-12-16 control licensing regulators ISP Internet service providers

NewsScan

# KEEP THE INTERNET NEUTRAL, SAYS LESSIG

Stanford Law School professor Lawrence Lessig says the time is ripe for regulators to take a stand on ensuring that access to the Internet remain neutral, and preventing access providers from controlling how consumers use the network. The Internet is essentially an "end-to-end" design, comparable to the electrical grid or the highway system, says Lessig. All the innovation comes from people using, not from the network itself. "But increasingly, U.S. broadband companies are trying to ensure that they have the power to decide which applications and content can run. Under such a regime, if Microsoft wants to sell Xboxes to run on the broadband network then it will have to pay the network providers for that privilege. Or if Disney wants to stream movies on the Internet, it too will have to pay the network tax," says Lessig. And while some people may think taxing Microsoft and Disney is not such a bad thing, the precedent it sets would stymie the growth and potential for innovation on the network. "It might seem strange that this lesson in preserving the original values of the Internet should come from Microsoft and Disney -- two companies that have suffered a great deal of criticism from network activists. But on this issue both deserve praise. Policymakers must see that what makes innovation possible on the Internet is the freedom to innovate without the permission of a network owner." (Financial Times 13 Dec 2002)

# 31.3 New technology with security implications

Category 31.3 New technology with security implications

2002-07-01 service bureau metered computing remote network

NewsScan

#### IBM PUTS A METER ON SOFTWARE USE

IBM is introducing a new service called Linux Virtual Services that enables customers to run a wide variety of software applications on IBM mainframes located in company data centers, and pay rates based largely on the amount of computing power they use. This metered payment system marks a major shift from the more conventional outsourcing and Web hosting arrangements typical today. IBM executive James Corgel touted the new service, saying "we see a huge opportunity going forward. Our best estimate is that in five years, 10% to 15% of the \$1 trillion IT market will be in the form of on-demand computing," with utility computing a significant part. Industry analysts remain a little more cautious about the prospects for metered computing. "We know customers are interested in doing this, but we don't know how many will," says one market researcher. Another added that "the pricing is still very complicated. It's not like electricity or even phone service." (Wall Street Journal 1 Jul 2002)

http://online.wsj.com/article/0,,SB1025472035492706880.... (sub req'd)

Category 31.3 New technology with security implications

2002-07-02 nanotechnology supercomputing data storage density

NewsScan

#### SPINTRONICS SHRINKS DATA STORAGE TO NANOSCALE

Researchers at the University at Buffalo in New York have developed a nickel-based, magnetic sensor, measuring only a few atoms in diameter, that could increase data storage capacity 1,000 times through the use of spintronics -- a field that takes advantage of electron spin as well as charge. Current technology used in data-reading sensors is based on giant magnetoresistance (GMR), where sensor resistance changes in a magnetic field. The new sensor developed at UB creates an effect called ballistic magnetoresistance (BMR), which uses an electrical conductor only a few atoms in size. Researchers say the technology could ultimately make it possible to store 50 or more DVDs on a hard drive the size of a credit card, or enable military personnel to carry supercomputers the size of a wristwatch into the field. (NewsFactor 1 Jul 2002) http://www.newsfactor.com/perl/story/18446.html

Category 31.3 New technology with security implications

2002-07-08 quantum computing nanotechnology brute force decryption encryption factoring public key cryptography PKC PKI

NewsScan

#### RACE IS ON BETWEEN QUANTUM ENCRYPTION AND COMPUTING

Dozens of labs around the world are working to develop the first viable quantum computer, but scientists note that the tremendous boost in computing power that these tiny machines will deliver could lead to chaos, as the majority of encryption schemes now used on banking, e-commerce and government Web sites would become instantly obsolete. Conventional encryption codes rely on the premise that the amount of time it would take for a computer to factor a multi-bit key makes them an unattractive target. "Now we have the challenge of turning quantum computation into an engineering reality," says MIT professor Isaac Chuang. "If we could perform this calculation at much larger scales -- say the thousands of qubits required to factor very large numbers -- fundamental changes would be needed in cryptography implementations." Quantum encryption is already being deployed on a limited basis in some military and intelligence applications, and in response, companies like MagiQ Technologies are working to develop quantum encryption products for commercial release. "Between the intrinsic weaknesses of classic cryptography and the advanced research and development -- both commercial and academic -- that is being conducted around the globe, quantum encryption will be a widespread security tool sooner than you may think," says MagiQ Technologies spokesman Andy Hammond, who predicts his company will have a "commercially available solution" in 2003. (Newsfactor Network 8 Jul 2002)

http://www.ecommercetimes.com/perl/story/18490.html

Category 31.3 New technology with security implications

2002-07-15 wireless technology broadband high speed download

NewsScan

#### NEW TECHNOLOGY REVS UP WIRELESS TRANSMISSIONS

The latest technology aimed at souping up wireless transmissions is Orthogonal Frequency Division Multiplexing (OFDM). Flarion Technologies, which is adapting OFDM for use on wireless networks, claims that in theory, at least, OFDM could enable a consumer to download an MP3 music album in eight minutes, compared with an hour and a half or more using today's technology. The OFDM technology faces an uphill battle to commercial adoption, however, because industry heavyweights have already invested billions of dollars in other standards such as GSM and CDMA. "It's not necessarily the best technology that wins," says a Yankee Group analyst. Meanwhile, OFDM will get its first trial run on a small section of Nextel's network, and Verizon, which tested Flarion gear in its labs last year, says it is monitoring the development as a possible way to improve the high-speed services it launched in January. Verizon said it was also keeping an eye on other OFDM developers, including BeamReach Networks, Malibu Networks and Broadstorm Telecom. (Reuters 14 Jul 2002)

Category 31.3 New technology with security implications

2002-07-29 satellite plane wireless telephone networks

NewsScan

#### SATELLITE PLANES IN OUR FUTURE?

A company called SkyTower hopes that within two or three years it will have satellite solar-powered planes flying over metropolitan areas to demonstrate the ability of such aircraft to serve as a low-cost platform for delivering a host of next-generation wireless services. An executive of AeroVironment, SkyTower's parent company, says: "We expect that within 10 years we can have thousands of airplanes in the sky over the major cities of the world. Development of the plane is basically finished." SkyTower got its name because the high-altitude aircraft can be though of as essentially a 12-mile tall tower that provides better coverage than satellites and terrestrial towers, since it would be both closer to earth than satellites and yet high enough to avoid ground interference from buildings and trees. (AP/San Jose Mercury News 29 Jul 2002)

Category 31.3 New technology with security implications

2002-08-13 nanotechnology transistors microprocessors

NewsScan

#### INTEL AIMS FOR LARGE-SCALE PRODUCTION OF NANOSCALE CHIPS

Intel is taking the wraps off a new technology that it says will enable it to produce the world's smallest transistors in large-scale production. This latest innovation is the result of Intel's \$12.5-billion spending spree over the last two years to improve manufacturing technologies and signals its intention to get a jump on rivals to be better positioned when the economy improves. The company's 90-nanometer production process entails a proprietary system for creating transistors whose key features are just 50 nanometers, or 1/2,000th of the width of a human hair. In addition, Intel is implementing a technology that effectively stretches the atoms apart in a silicon wafer to allow electrical current to flow faster, boosting performance, and is moving forward with plans to shift over to the 12-inch (300-milimeter) silicon wafer standard, up from the current eight inches. (Wall Street Journal 13 Aug 2002)

Category 31.3 New technology with security implications

2002-08-19 laptop computers fuel cells portable digital divide international development

NewsScan

#### THE EVER-EVOLVING LAPTOP

Laptop computers are making significant inroads in the computer market, with notebook growth pegged at 6% in the second quarter, despite a decline in overall sales. And while desktop machines are not likely to change much in style over the next few years, the laptop of the future will be smaller, lighter, and may even run on methane. PolyFuel, a spinoff of SRI International, is developing fuel cells that break down methane molecules into protons, electrons and carbon dioxide. While the protons pass through a special membrane, the electrons are maneuvered into a wire that powers the laptop. The replacement fuel cartridges initially will last two to three times longer than conventional batteries but eventually will last 10 times longer. Other companies are seeking to expand battery life by supplementing them with supercapacitators, which store energy at the chip level. "Supercapacitators hold more electricity than capacitators and transfer and recharge faster than batteries," says Anthony Kongats, CEO of supercapacitator startup Cap-XX. Batteries can be completely removed and the notebook will continue to run for about five minutes. Supercapacitator-enhanced notebooks could begin hitting the shelves in 2004 and notebooks powered by fuel cells could be available by late 2004 to 2005. Other likely laptop improvements include wireless capability that can switch effortlessly between WiFi and cellular networks, as well as low-power screens and new types of heat-dissipation techniques. (CNet News.com 19 Aug 2002)

http://news.com.com/2100-1001-951449.html?tag=fd\_lede

Category 31.3 New technology with security implications

2002-09-03 large-capacity disk recorder download copyright infringement piracy movies TV

television

NewsScan

#### SONY TAKES THE WRAPS OFF 'COCOON'

Sony unveiled the first of its "Cocoon" line of products that aim to replace the PC for downloading Internet content. The new video recorder sports a 160-gigabyte hard-disk, capable of recording up to 15 hours of HDTV or up to 100 hours of standard quality programming. It features an always-on broadband Internet connection that enables to access programming information online and records TV programs that match preferences selected by the owner. It can also "infer" preferences from previously recorded content and automatically record programs that fit that profile. The device even offers an apology if the owner rejects its selections. The new system will roll out in Japan on Nov. 1, but Sony has not yet said when it will be available for sale overseas. Cocoon is based on the Linux platform and will be priced at about \$1,100. (Reuters 4 Sep 2002)

Category 31.3 New technology with security implications
2002-09-09 nanotechnology memory chip logic

NewsScan

#### HP DESIGNS NANOSCALE MEMORY CHIPS

Hewlett-Packard has created a new computer memory chip using nanotechnology to fit a 64-bit memory unit inside a single square micron (a micron is one-millionth of a meter). Although the new chip's capacity is too small to be useful, the development signals a key advance in the prevailing trend toward miniaturization. In addition, the chip combines for the first time both memory and logic by manipulating molecules caught in a grid of superthin platinum wires. "This is the first demonstration that molecular logic and memory can work together on the same nanoscale circuits," says an HP spokesman. (CNN.com 9 Sep 2002)

Category 31.3 New technology with security implications

2002-09-11 nanotechnology transistors microprocessors

NewsScan

### AMD UNVEILS TINY DOUBLE-GATE TRANSISTORS

Advanced Micro Devices reports that it has succeeded in manufacturing the smallest double-gate transistors to date using industry-standard technology. The gate of the transistor, across which electrical current flows to turn the switch on, measures 10 nanometers, or 10 billionths of a meter. AMD says this latest development means that a chip now capable of holding 100 million transistors could conceivably pack about a billion of the nanoscale transistors. (Reuters/Los Angeles Times 11 Sep 2002)

Category 31.3 New technology with security implications

2002-09-18 transistor nanotechnology computer performance speed

NewsScan

#### INTEL DEVELOPS 'TRI-GATE' TRANSISTOR

Intel has developed a 'tri-gate' transistor, planned for large-scale production after 2005, which uses three rather than the current single logic gate, in order to increase computer performance The company says the new technology amounts to a three-dimensional extension of the terahertz transistor architecture it has already presented at research conferences. (Reuters/San Jose Mercury News 17 Sep 2002)

Category 31.3 New technology with security implications

2002-10-07 palm pocket handheld computer low cost available

NewsScan

#### PALM WILL OFFER A HANDHELD FOR \$99

Staking out a position in the low end of the handheld computer market, Palm is offering an entry-level device for \$99. Called the Palm Zire, it's made in China for less than \$80. Industry analyst Tim Bajarin of the Creative Strategies consulting firm says Palm's low-end strategy has a pretty good chance of succeeding: "Palm should have this part of the market to themselves for actually quite a while. It's pretty much a win-win for Palm, for Palm software partners, for Palm after-market partners." Sony and Handspring, the No. 2 and No. 3 handheld manufacturers, also use the Palm operating system, are focused on the higher end of the market, and the companies that license Microsoft Pocket PC software usually charge \$300 or more for their products. (San Jose Mercury News 6 Oct 2002)

Category 31.3 New technology with security implications

2002-10-17 location surveillance wireless beacon

NewsScan

#### NOAA EXPANDS 'PERSONAL LOCATOR BEACON' PROGRAM

Beginning July 1, the National Oceanic and Atmospheric Administration will extend to hikers, hunters and other land-bound recreational enthusiasts the same emergency locator service now available to pilots and boaters. The "personal locator beacons" -- handheld devices equipped with GPS technology -- work in zones not covered by cell phone networks and will cost \$300 or more. "It takes the search out of search and rescue," says Randy Crosby, who heads up rescue teams in northern Alaska, where the devices have been tested for the past six years. In its 20 years of operation, the satellite rescue system has helped save some 14,000 people worldwide, including about 4,300 in the U.S. There is no penalty for accidental false alarms, but deliberate misuse can cost perpetrators up to \$250,000 in fines, a six-year prison term and reimbursement of rescue costs. NOAA spokesman Daniel Karlson says the government works to educate beacon owners so "someone doesn't go out there and stub their toe and trip this thing off. We want this as a last resort. (AP 16 Oct 2002) http://apnews.excite.com/article/20021016/D7MMLK0O0.htm

Category 31.3 New technology with security implications

2002-10-22 Wi-Fi wireless communication mobile computing strategies plans predictions

NewsScan

#### INTEL BETS BIG ON WI-FI

Intel is investing \$150 million in companies involved in developing Wi-Fi technology, in the chipmaker's latest strategy to stimulate markets that could boost demand for its chips. Intel plans next year to introduce a chip technology for mobile computing -- code-named Banias -- that offers built-in Wi-Fi capability. The top three areas targeted for investment by Intel will be: companies helping to expand the number of Wi-Fi-equipped locations or otherwise helping to improve wireless infrastructure; companies working to solve some fundamental problems associated with the technology; and companies that improve the basic capabilities of the technology. The company plans to allocate the money for wireless investments from an existing \$500 million communications fund. (Wall Street Journal 22 Oct 2002)

#### MOBILE PC SALES Another note on Intel's interest in Wi-Fi:

Melissa McVicker, the company's Asia Pacific regional manager, says that sales of mobile PCs are set to grow at a compounded rate of 15% to more than 50 million units by 2006 (compared to 30 million in 2002), and nine out of ten of them will make use of Wi-Fi or other wireless network technology. She says that "countries like Japan and Korea have about 50% of their PC purchases in mobile PCs, and there are a few others in Asia that are moving up quickly." Global demand for mobile PCs such as laptops and notebooks will soon outpace demand for desktop systems. (Reuters/San Jose Mercury News 22 Oct 2002)

Category 31.3 New technology with security implications

2002-10-28 fast computing devices nanotechnology

NewsScan

### LIGHT-EMITTING SILICON BREAKTHROUGH

STMicroelectronics, the world's largest chip maker after Intel and AMD, has made a breakthrough in light-emitting silicon that could lead a new generation of more-powerful computing devices and higher-speed optical data-transmission systems. The efficiency of light-emitting silicon has been increased 100-fold, according to the researchers who achieved the breakthrough. Technology consultant Richard Doherty of Envisioneering says, "As we move toward placing entire computing systems on a single chip, the need to optically clock microelectronic circuits will become crucial." (New York Times 28 Oct 2002)

Category 31.3 New technology with security implications

2002-12-04 e-commerce intellectual property distribution subscriptions

NewsScan

# MOVIE SUBSCRIPTIONS OVER THE NET

RealNetworks, the software company specializing in the digital distribution of music and video over the Internet, and StarZ, the cable company, have teamed up to offer movie subscriptions over the Internet. Customers will pay about \$10 a month, and will receive movie downloads suitable for viewing on computer displays; customers wanting to view the movies on a TV screen would need additional equipment. (AP/San Jose Mercury News 4 Dec 2002)

http://www.siliconvalley.com/mld/siliconvalley/4661968.htm

Category 31.3 New technology with security implications

2002-12-05 digital divide broadband ISP Internet service provider dialup modem

NewsScan

#### BROADBAND: FAST BUT PRICEY -- APPARENTLY TOO PRICEY

Although 70% of U.S. households now have the technical option of subscribing to broadband services, only15% actually do, because many people are intimidated by the high cost of broadband: typically \$40-50 a month, whether it is acquired through cable company or phone company. The problem is an upscale corollary of basic theorem of the digital divide, and is illustrated by the fact that whereas 28% of households with income above \$100K a year have broadband access, a mere 4% of families with household incomes under \$35K a year have such access. The industry is trying to reconcile itself to the basic facts of economic life; analyst Daryl Schoolar of the InStat/MDR research firm says: "We're working with a model of broadband adoption that is long and steady, rather than a big revolutionary pop." Which means that most network users will still be using dial-up connections a long, long time from now. Professor Andrew Odlyhzko of the University of Minnesota says all this is not too surprising: "There is hardly anything more ludicrous than the fax machine, but it is still around." (New York Times 5 Dec 2002)

http://partners.nytimes.com/2002/12/05/technology/05BROA.html

Category 31.3 New technology with security implications

2002-12-07 wireless networks Internet access growth Wi-Fi

NewsScan

#### AT&T, IBM AND INTEL FORM WI-FI VENTURE

AT&T, IBM and Intel are teaming up to back a new venture, called Cometa Networks, which plans to deploy a nationwide Wi-Fi wireless data network in coffee shops, hotels and other public venues. Cometa CEO Larry Brilliant says his company's goal is to install a wireless antenna within five minutes of anyone located in the top 50 U.S. metropolitan areas. A company spokeswoman says Cometa's advantage over the current informal hodgepodge of Wi-Fi hot spots is that it will offer "consistent, uniform service at a variety of locations. We think this is an important marketplace." Yankee Group analyst Roberta Wiggins says the involvement of the three industry heavyweights "obviously gives credibility to this whole arena." (Wall Street Journal 6 Dec 2002)

http://online.wsj.com/article/0,,SB1039109828499400393.djm,00.html (sub req'd)

# 32.1 Censorship in the USA

Category 32.1 Censorship in the USA

2002-03-25 library Internet content filtering software children censorware legal challenge lawsuit

NewsScan

#### LEGAL CHALLENGE TO CHILDREN'S INTERNET PROTECTION ACT

A coalition of libraries, Web sites and other interested parties has begun offerings testimony in court hearings on the constitutionality of the Children's Internet Protection Act of 2000, which requires public libraries that accept federal financing or technology discounts to install software filters to protect children from adult material on the Internet. In the words of Senator John McCain (R-Ariz.), the law passed by Congress is intended to allow "local communities to decide what technology they want to use, and what to filter out, so that our children's minds aren't polluted." Coalition members include the American Library Association, the American Civil Liberties Union, and one Republican lawmaker who had originally supported the legislation but changed his mind about it when he discovered that his own campaign site was blocked out by one popular filtering program. (New York Times 25 Mar 2002)

http://partners.nytimes.com/2002/03/25/national/25LIBR.html

#### PROTECTING CHILDREN OR ABRIDGING FREE SPEECH?

A second week of testimony has begun [April 2, 2003] in Philadelphia in a federal district court that is hearing a case to decide a constitutional challenge to the Children's Internet Protection Act (CIPA), signed by President Clinton in 2000 and intended to protect children from violence and pornography without abridging the free-speech rights of adults. Shown a ring binder filled with pornographic images and asked by a government attorney, "Is it your testimony that I have the right to look at these Web pages?" librarian Candace Morgan said "Yes, it is," and added later: "We have sex manuals with similar pictures to this one." Another witness, Chris Lemmon, said he found pornographic sites involving elderly women "disturbing." The plaintiffs in the case are arguing, among other things, that CIPA relies on technology that can not distinguish between protected and unprotected speech. The government's position is that libraries that don't want to use software filters to protect children can simply refuse to accept federal subsidies since CIPA applies only to institutions that receive government funding. (AP/Washington Post 1 Apr 2002)

http://www.washingtonpost.com/wp-dyn/articles/A47070-2002Apr1.html

#### COURT OVERTURNS LAW REQUIRING SOFTWARE FILTERS

A three-judge federal panel in Philadelphia struck down a provision of the Children's Internet Protection Act (CIPA) requiring public libraries to install software on library terminals to filter out pornographic material. The law applied to libraries that received federal technology funding, and supporters of the law had maintained that Congress has the right to decide what it does or doesn't want to fund. But the Court ruled that the legislation was fatally flawed because there currently exists no software that can with complete precision filter only the targeted material -- and nothing else by accident. The case is likely to be appealed to the U.S. Supreme court. (San Jose Mercury-News 1 Jun 2002) http://www.siliconvalley.com/mld/siliconvalley/3379690.htm

Category 32.1 Censorship in the USA

2002-04-05 library Internet content filtering software children censorware legal challenge lawsuit

NewsScan

#### LIBRARY NET PORN CASE WILL BE APPEALED REGARDLESS OF OUTCOME

A decision from the three-judge federal appeals court in Philadelphia hearing the dispute over the constitutionality of the Children's Internet Protection Act (CIPA) will be handed down next month [May 2002], but is certain to be appealed to the Supreme Court, no matter how the judges decide. One of the judges observed, "We're stuck right in the heart of the First Amendment when we're talking about libraries." Another judge, concerned that decisions on what constitutes pornography were being left to "nameless and faceless" people in software filtering firms, asked "What right does the government have to require this kind of filtering system?" (CIPA requires libraries that accept federal funding to use such systems to protect children from pornography and violence.) Critics charge that the software filters are blunt instruments that cannot reliably discern the difference between pornography and constitutionally protected information. An ACLU lawyer calls the law "a sham," since "everybody knows you can't comply with its terms." A Justice Department lawyer sees the issues differently: "There is no constitutional right to immediate, anonymous access to speech, for free, in a public library." And then adds: "Even if you assume that libraries have a right to provide unfettered access to the Internet, they don't have a right to do so with a federal subsidy. The crux of this matter is whether or not Congress has the power to decide how to use its money." (Reuters/USA Today 4 Apr 2002)

http://www.usatoday.com/life/cyber/tech/2002/04/04/library-porn.htm

Category 32.1 Censorship in the USA

2002-04-12 computer games standards monitoring labeling censorship children commerce

regulation ratings

NewsScan

#### FTC SCRUTINIZES 'MATURE' VIDEO GAMES

The Federal Trade Commission has requested information on sales of mature-themed video games to minors, as a precursor to an expected June report on media violence. In December, the FTC issued a report that offered four suggestions for the movie, music and games businesses: establish industry standards on advertising in places where the primary audience is under 17; develop better labeling of ratings within ads; improve self-regulation with regard to retailer compliance; and implement industry sanctions for non-compliance with sales and advertising sanctions. Since the video game rating system was instituted in 1994, more than 7,000 games have been rated, with some 500 earning an "M" (mature) rating, meaning they are not intended to be played by children under 17. (Reuters/USA Today 11 Apr 2002)

http://www.usatoday.com/life/cyber/tech/2002/04/11/ftc-video-games.htm

Category 32.1 Censorship in the USA

2002-04-17 virtual child pornography free speech SCOTUS lawsuit ruling judgement decision

constitution

NewsScan

#### COURT SAYS THAT TO HAVE CHILD PORNOGRAPHY YOU NEED A CHILD

The U.S. Supreme Court has ruled that portions of the Child Pornography Prevention Act of 1996 are unconstitutional because they infringe on First Amendment free-speech rights. (In U.S. law, images have traditionally been considered a form of "speech.") The 1996 law banned "virtual" pornography that uses computer-manipulated images rather than real children to portray children engaged in sex acts. Justice Anthony M. Kennedy wrote in the majority opinion that the government "has shown no more than a remote connection between speech that might encourage thoughts or impulses and any resulting child abuse. The mere tendency of speech to encourage unlawful acts is not a sufficient reason for banning it." (New York Times 17 Apr 2002)

http://partners.nytimes.com/2002/04/17/national/17PORN.html

Category 32.1 Censorship in the USA

2002-04-26 parental consent violent sexual videogames free speech legal judgement

NewsScan

#### JUDGE SAYS GOVERNMENT'S [CAN] RESTRICT KIDS' ACCESS TO VIDEO GAMES

Remarking that "video games have more in common with board games and sports than they do with motion pictures," U.S. District Judge Stephen Limbaugh has ruled in support of a St. Louis County ordinance requiring children under 17 to have parental consent before they can buy violent or sexual videogames (or play such games in video arcades). Judge Limbaugh believes the ruling had nothing to do with free speech, because the games provide "no conveyance of ideas, expression, or anything else that could possibly amount to speech." The Interactive Digital Software Association, which had challenged the ordinance, plans to appeal the ruling, asserting that it "is clearly in conflict with virtually every other federal court decision on this and related issues." (AP/USA Today 24 Apr 2002)

http://www.usatoday.com/life/cyber/tech/2002/04/24/judge-games.htm

Category 32.1 Censorship in the USA

2002-05-07 video games sex violence standards proposed legislation law

NewsScan

#### BILL WOULD BAN SALE OF VIOLENT VIDEO GAMES TO KIDS

California Congressman Joe Baca has proposed legislation that would ban to children sales of video games that contain scenes of decapitation and dismemberment, murder, car jackings, illegal drug use, rape, prostitution, assault and other violent crimes. Doug Lowenstein, president of the Interactive Digital Software Association, thinks the bill is "both unnecessary and unconstitutional," but acknowledges: "I certainly respect the concerns that give rise to a bill like this." In introducing the legislation Congressman Baca said: "I've had enough of the violence we're experiencing among our youth. When kids play video games, they assume the identity of the characters in the games ... Do you really want your kids assuming the role of a mass murderer or car jacker when you are away at work?" (Reuters/San Jose Mercury News 6 May 2002) http://www.siliconvalley.com/mld/siliconvalley/3210541.htm

Category 32.1 Censorship in the USA

2002-05-14 COPA pornography content filterining constitutionality legal challenge

NewsScan

Category 32.1

#### CHILD ONLINE PROTECTION ACT SURVIVES REVIEW (JUST BARELY)

Censorship in the USA

The Child Online Protection Act, passed by Congress in 1998 and intended to impose prison sentences for posting material "harmful to minors" on a Web site to which minors could have access, survived a lower court ruling that had declared it unconstitutional. The lower court's decision hinged on its rejection of a clause in the Act defining "objectionable" material as material that did not meet "contemporary community standards," a definition which the lower court said would give veto power over the Internet to "the most puritan of communities." The appellate court thought that point settled the matter, but the Supreme Court sent the case back to Federal District Court with instructions to think through all of the relevant issues before making a decision. Court-watchers expect that the Act will eventually be declared unconstitutional by the Supreme Court, when the lower court is finished reconsidering it. (New York Times 14 May 2002) http://www.nytimes.com/2002/05/14/national/14SCOT.html

2002-05-17 **COPA SCOTUS ruling** 

FindLaw ConstitutionalCaseLaw, http://laws.lp.findlaw.com/us/000/001293.html

SCOTUS: ASHCROFT v. AMER. CIVIL LIBERTIES UNION (05/13/02 - No. 00-1293)

The Child Online Protection Act's (COPA) use of "community standards" to identify what material "is harmful to minors" does not by itself render the COPA statute substantially overbroad under the First Amendment.

To read the full text of this opinion, go to:

Category 32.1 Censorship in the USA

2002-05-28 videogames indecency violence gore obscenity standards restrictions ratings

FindLaw Download This 87

# OF DOOM, GLOOM, FUN AND GAMES

Video games and their designers are all grown up, ready to take on darker, mature themes. The change hasn't slowed their popularity with fans, but it has given lawmakers pause. . . Earlier this month, a federal judge in St. Louis upheld a county law that criminalized the sale of "Mature"-rated video games to anyone under 17, despite the lack of similar laws that would punish the sale of R-rated movies or CDs with parental warnings to those same kids. "I think the root of the problem is that most observers do not yet appreciate the fact that video games are artistic achievements every bit as worthy and creative as a film, a song or a painting," said Douglas Lowenstein, IDSA's president.

http://www.wired.com/news/games/0,2101,52661,00.html

Interactive Digital Software Association

http://www.idsa.com/

Category 32.1 Censorship in the USA

2002-05-28 Web free speech censorship decency violence gore law enforcement police

FindLaw Download This 87

#### UNDER FBI PRESSURE, SITE REMOVES PEARL MURDER VIDEO

Saying it was under pressure from the FBI, a Web site that specializes in gruesome images has removed video footage recorded during Wall Street Journal reporter Daniel Pearl's murder. The operator of the Ogrish.com site and the president of its Web hosting company told Newsbytes the FBI ordered the video taken down under threat of a lawsuit, but a spokeswoman for the FBI said the bureau merely made a "courtesy request" on behalf of Pearl's family.

http://www.newsbytes.com/news/02/176762.html

The Daniel Pearl Foundation

http://www.danielpearlfoundation.org/

Category 32.1 Censorship in the USA

2002-06-04 SCOTUS virtual child pornography

FindLaw Download This 88

#### SOLVING KID PORN'S 'REAL' PROBLEM

In the aftermath of a U.S. Supreme Court ruling that computer-generated images of minors engaged in sexual acts are not illegal and are in fact protected by the First Amendment, some prosecutors and police investigators have found themselves at a loss for how to proceed in child porn cases. More suspects are claiming that the seemingly illicit pictures and videos found on their hard drives are ersatz, police say. And an Illinois man who had already pleaded guilty to possessing 2,600 images of kiddie porn was freed from jail when a judge ruled that the state's law was unconstitutional because it failed to distinguish between real and fake porn. http://www.wired.com/news/business/0,1367,52945,00.html

Read the Opinion (AMERICAN LIBRARY ASS'N., INC. v. US)[PDF]

http://news.findlaw.com/hdocs/docs/ala/cipa53102opn.pdf

View the Order Enjoining the Enforcement of the CIPA [PDF] http://news.findlaw.com/hdocs/docs/ala/cipa53102ord.pdf

Category 32.1 Censorship in the USA

2002-06-19 Internet content filters pornography software workarounds exploits

NewsScan

#### THE FILTER WARS

Arguing that "intellectual development is one of the fundamental human rights and it's also a right that people under 18 have," programmer Bennett Haselton has made a reputation as a foe of software filters designed to shield children from pornography and violence. He's created an organization called Peacefire.org, which offers free downloads and details methods for getting around filtering software. Haselton says, "This is something that practically nobody else is working on, and only a couple of people in the world actually know as much about the blocking software issue." One of Haselton's many critics, Marc Kanter of Solid Oak Software, which makes the popular CYBERsitter filtering program, says of him: "He's being totally irresponsible. When he started Peacefire, he was a kid himself. Basically he was enticing minors into his beliefs and activities, which was to undermine parents' rights. As an adult now, he should know better than that." (AP/USA Today 17 Jun 2002) http://www.usatoday.com/life/cyber/tech/2002/06/18/net-filter-war.htm

Category 32.1 Censorship in the USA

2002-06-20 child pornography legislation law proposal digital photography simulations free

speech censorship

NewsScan

# CONGRESS GETS READY TO CONTINUE FIGHT AGAINST KID PORN

If at first you don't succeed, try, try again, and the House Judiciary Committee is trying once again to write legislation that will not only ban virtual child pornography but also pass Supreme Court muster. The new, more narrowly drafted bill would outlaw child pornography involving any prepubescent child, including computer images of such a child if the images were indistinguishable from actual photos. New York Democrat Jerry Nadler argued against the bill, on the grounds that it would criminalize protected speech, but fellow Democrat Adam Schiff, a Californian, insisted: "If we only go after pornography using real children we will effectively preclude any real prosecution of child pornography." (Reuters/USA Today) http://www.usatoday.com/life/cyber/tech/2002/06/19/virtual-porn.htm

Category 32.1 Censorship in the USA

2002-11-18 children video games violence ethics crime education pornography theft

NewsScan

# CRIME PAYS

The new videogame "Grand Theft Auto: Vice City" sold more than 1.4 million copies the first two days it was available, at an average of \$48 a copy. Chock full of violence, prostitutes and porn stars, it is probably the fastest-selling game in the 20-year history of the videogame industry. (USA Today 18 Nov 2002)

# 32.2 Censorship outside the USA

Category 32.2 Censorship outside the USA

2002-02-22 ISP Internet service providers hate speech censorship international regulation

agreement treaty harmonization cooperation law enforcement investigation prosecution extradition

NewsScan

# EUROPEAN "HATE SPEECH" LEGISLATION WORRIES CIVIL LIBERTARIANS [22 Feb 2002]

A proposal by the Council of Europe that would criminalize racist and other "hate speech" on the Internet is worrying both civil libertarian groups (which regard it as a blow against free speech) and Internet service providers (which are concerned about their legal liability for material posted without their consent). The principal administrator of the Council of Europe thinks that the various countries belonging to the organization must "harmonize" their laws "so that countries can cooperate in criminal investigations regarding the Internet," but the head of the Campaign Against Censorship on the Internet in Britain took a very different view: "This proposal could potentially outlaw free speech. That would be a great infringement of civil rights." (Reuters 22 Feb 2002)

http://www.reuters.com/news\_article.jhtml?type=internetnews&StoryID=623493

Category 32.2 Censorship outside the USA

2002-05-16 international censorship Great Firewall of China content filtering

NewsScan

#### CHINA SUSPENDS CENSORSHIP OF WESTERN NEWS SITES

Without explanation, the Chinese government has removed blocks on the normally censored foreign Web sites, including those of such news organizations as Reuters, CNN and the Washington Post. It is not known whether the decision would stay in force, and officials at the International Press Centre and the Ministry of State Security provided no information about the new development. The Web sites of the Los Angeles Times, National Public Radio, the San Francisco Chronicle, the Boston Globe, and the Atlanta Journal-Constitution can also now be accessed, whereas the Time magazine, Voice of America, and BBC News sites still appear to be blocked. (Reuters/San Jose Mercury News 15 May 2002) http://www.siliconvalley.com/mld/siliconvalley/3273080.htm

Category 32.2 Censorship outside the USA

2002-09-12 government censorship international search engine Web content filtering firewall

NewsScan

# WHERE IN THE WORLD IS GOOGLE? HINT: NOT CHINA

As part of a wider clamp-down on the ability of Chinese citizens to use the Internet to learn about the world beyond the country's "Great Firewall," Chinese authorities have blocked access to Google. The Google search engine is especially popular in China because it can run Chinese-language searches. (San Jose Mercury News)

#### CHINA ENDS BLOCKING OF GOOGLE

Chinese authorities have ended their policy of preventing citizens in that country from accessing the Google search engine, which is especially popular there because of its ability to make it easy to find Chinese-language material online. In its usual style, the government gave no indication of why it was removing the restrictions (nor, for that matter, why it had imposed them in the first place). But censorship in China continues, as evidenced by an increase in selective blocking, which prevents visitors to a Web site from seeing specific items which the government finds politically incorrect. (AP/San Jose Mercury News 12 Sep 2002)

Category 32.2 Censorship outside the USA

2002-10-25 censorship legal restrictions free speech hate search engine Web

NewsScan

#### GOOGLE CENSORS SEARCH RESULTS FOR FRENCH AND GERMAN USERS

A report from Harvard Law School found that when users from France and Germany tap Google's search engine, at least 100 sites are automatically deleted from the search results. Most of the missing sites promote either white supremacy or Holocaust denial. Both France and Germany have strict laws banning hate speech, and a Google spokesman says the company must occasionally remove sites to avoid legal liability. Such removals are done in response to specific requests and are not done preemptively, he added. "We carefully consider any credible complaint on a case-by-case basis and take necessary action. We only react to requests that come to us." Harvard Law School researchers found about 65 sites that were excluded from Google.de, the German site, and about 113 sites were missing at Google.fr, the French site. (AP 24 Oct 2002) http://apnews.excite.com/article/20021024/D7MS6SJ80.htm

Category 32.2 Censorship outside the USA

2002-12-04 censorship international regulations Internet access content filtering firewall

pornography politics

NewsScan

#### LAND OF THE CENSOR: CHINA

A study by Harvard Law School researchers finds that China is the country with the world's most oppressive censorship of what its citizens can view on the Internet. Chinese authorities block access to 19,000 sites, and also delete individual links or Web pages of which they do not approve. Most of the disapproved sites are political in nature. When it comes to blocking pornography, China (at least for now) cedes the first-place prize to Saudi Arabia: China blocks fewer than 15% of sexually explicit Web sites compared to Saudi Arabia's blocking of 86%. (New York Times 4 Dec 2002) http://partners.nytimes.com/2002/12/04/international/asia/04CHIN.html

#### CENSORSHIP IN CHINA: WHAT ARE THEY THINKING?

We've previously reported that Chinese officials have the most stringent Internet censorship program in the world, but haven't remarked on the broad scope of it. It blocks out not only pro-democracy content but also a bit of just about everything else. Jonathan Zittrain and Benjamin Edelman, two Harvard Law School researchers who have been studying international Internet filtering, say that in addition to Taiwanese and Tibetan pro-democracy sites the Chinese also block health sites, U.S. university sites, and sites devoted to comic books, science fiction, etc. Human rights worker Greg Walton comments: "The study's an interesting insight into the Chinese censor's head. If I was a psychologist and I had China's censor on the couch, I'd ask, 'Why are you repressing these things?"" (Wired News 4 Dec 2002) http://www.wired.com/news/politics/0,1283,56699,00.html

Category 32.2 Censorship outside the USA

2002-12-20 censorship arrest writer freedom speech international

NewsScan

# CHINESE AUTHOR ARRESTED AFTER INTERNET CRACKDOWN

The novelist and poet Liao Yiwu, who has written about the very poorest social strata in China, is one of several dozen activists detained by law enforcement authorities in the city of Chengdu in southwestern China. Liao's articles about the poor are banned in China but have been published abroad by Web sites critical of the Chinese regime. (USA Today 19 Dec 2002)

Category 32.2 Censorship outside the USA

2002-12-31 video games sex pornography violence age children adults

NewsScan

#### EUROPEAN UNION TO RATE VIDEO GAMES FOR SEX AND VIOLENCE

Violent and sexually-oriented computer games sold in Europe will soon be getting classifications established by the European Union: games with no sex or violence at all will get a rating of 3+ and all other games will receive ratings of 7+, 12+, 16+, or 18+. EU secretary-general Patrice Chazerand says: "It is only fitting that an industry exerting increasing influence on people displays an enhanced sense of social responsibility." (BBC News 29 Dec 2002)

http://news.bbc.co.uk/1/hi/technology/2612983.stm

# 33.1 Acceptable use policies

Category 33.1 Acceptable use policies

2002-01-20 Internet content filtering students schools portable games music piracy instant messaging appropriate use policy

NewsScan

#### VIRGINIA COUNTY RECALLS STUDENT LAPTOPS [20 Jan 2002]

Henrico County, Va. school officials are recalling all 11,000 laptop computers that it distributed to its high school students in order to retrofit them with security software that will prevent students from using the devices for accessing pornography or changing their grades -- abuses that reportedly have occurred since the machines were handed out last fall. Game and music downloading capabilities will also be eliminated or heavily restricted and instant messaging will be limited to home use. Teachers have complained that in-class use of entertainment file-sharing and messaging are disruptive. (AP/Wall Street Journal 20 Jan 2002)

http://interactive.wsj.com/articles/SB1011563803808773240.htm

Category 33.1 Acceptable use policies

2002-03-22 e-mail user interface management reliability productivity

NewsScan

#### A GOOSE AND GANDER STORY: AOL TIME WARNER WORKERS HATE AOL MAIL SYSTEM

When AOL and Time Warner merged, executives of the new company required the divisions of the old Time Warner to adopt AOL mail system for internal use throughout the new company. But now that policy has been reversed, because managers and employees complained bitterly that AOL's consumer-oriented system is unfit for serious business use, maintaining that the software crashes, messages can't handle large attachments, communications sent to large groups of people are mis-identified as spam and thrown away, and so forth. Staffers in Time's Washington bureau apparently began to mock the AOL mail system by singing out, "So easy to use, no wonder it's number one." So employees began relying less on e-mail and more on other forms of communication. One staffer said, "If all goes well, we'll never have to use e-mail and we'll start talking to each other again." (Wall Street Journal 22 Mar 2002)

http://www.online.wsj.com/ (sub req'd)

Category 33.1 Acceptable use policies

2002-03-28 free speech property e-mail corporation employee lawsuit SCOTUS

NewsScan

#### CALIFORNIA CASE PITS SPEECH RIGHTS VS. PROPERTY RIGHTS

The California Supreme Court has agree to review a case involving a disgruntled Intel employee who sent 30,000 e-mail messages to company employees at their places of work. The employee, backed by the American Civil Liberties Union and the Electronic Frontier Foundation, sees the case as one raising fundamental free speech rights denied to an individual who wished to circulate his opinion; in contrast, the lower courts have viewed it as a property-rights case, since the messages were sent not to employees at their homes but to their company e-mail addresses. The appellate court's majority ruled that "Intel is as much entitled to control its e-mail system as it is to guard its factories and hallway." A dissenting opinion argued that it could be considered a property-rights case only if Intel had shown that its property had actually been harmed, and there was no such showing. (San Jose Mercury News 27 Mar 2002)

http://www.siliconvalley.com/mld/siliconvalley/2948781.htm

Category 33.1 Acceptable use policies

2002-08-02 e-mail content inspection limits regulations rules employee employer policy suitability

31

#### NewsScan

# LAWSUIT OVER CONTENT OF EMPLOYEE E-MAIL

The Virginia-based nonprofit American Center for Law and Justice has filed a lawsuit against a Dallas school district over its policy restricting the content of employee e-mail messages. The policy allows employees to send "work-related" or "private" messages -- but does not allow "religious worship" or "proselytizing." The suit is being filed on behalf of a female employee who was threatened with having her e-mail privileges suspended after she sent e-mail with religious content to her friends. (AP/San Jose Mercury News 1 Aug 2002)

Category 33.1 Acceptable use policies

2002-08-30 availability prompt response policy e-mail customer relations management CRM

NewsScan

#### COMPANIES LAX ON ANSWERING E-MAIL

Companies' efforts to shift customer relationship management to the Web and e-mail may backfire unless they institute a prompt response mechanism, says a new study by Jupiter Research. Only half of the companies surveyed responded to a customer's question or issue within 24 hours, while a third took three days or longer. "That lack of response could drive consumers back to more costly channels such as the telephone," says Jupiter analyst David Daniels. "Consumers are definitely concerned about this." And while self-service is catching on with consumers savvy enough to navigate their way through a Web site, companies should be cautious about relying on it too heavily. "Self-service really lends itself to commodity goods categories (like books or CDs). When it gets up into more complicated situations, such as computing products or wireless phones, consumers absolutely said they want a real-time solution. Those frequently-asked-question lists are not necessarily specific enough to meet their needs," says Daniels. (CNet News.com 29 Aug 2002) http://news.com.com/2100-1017-955947.html?tag=fd\_top

Category 33.1 Acceptable use policies

2002-10-25 copyright intellectual property piracy corporate policy

NewsScan

#### HOLLYWOOD GOES TO WORK TO STOP DIGITAL PIRACY

Hollywood studios and record companies are asking the heads of U.S. corporations to prevent their employees from using high-speed company networks to download copyrighted material from peer-to-peer services such as Kazaa and Gnutella which are used to exchange songs and movies. The letter sent by these groups suggests that businesses could be held liable for the copyright infringements made by their workers. (Reuters/USA Today 25 Oct 2002)

Category 33.1 Acceptable use policies

2002-11-26 university policy copyright infringement intellectual property student seizure

NewsScan

#### NAVAL ACADEMY SEIZES STUDENT COMPUTERS FOR ILLEGAL COPYING

The U.S. Naval Academy in Annapolis, Maryland, has seized about one hundred student computers it suspects were used to receive illegally downloaded music and movies. Guilty students could receive punishments ranging from loss of leave time to court-martial and expulsion -- far stricter punishments than are meted out to civilian students who are not charged with misusing federal property. It is not uncommon for students to be oblivious, indifferent, or positively hostile to the notion that it is wrong to steal copyrighted material. One student at an east-coast university says of music and video file-copying, "This is a lot better deal than going out and spending \$15 for twenty other tracks on a CD you don't want. It takes you 5 or 10 seconds to type in. There's no risk, and it's one of those things where you don't see the victim." (Washington Post 26 Nov 2002)

# 33.2 Spam

Category 33.2 Spam

2002-01-08 viral marketing e-mail chain letter consumer spam junk e-mail worm social

engineering

NewsScan

#### VIRAL MARKETING GOES MAINSTREAM

Viral marketing is set to invade your in-box, say advertisers who are looking to this upstart marketing method to boost their outreach efforts. "At the moment, say 'viral marketing' and you still think teens and fashion brands -- cool things for cool people distributed via e-mail. But the principles that make viral marketing work should be taken on board by any brand-owner wanting to target any age group," says marketing consultant David Nichols. "Grown-up viral marketing is about involving people in things they love as a way of introducing a dialogue between brand and consumer." E-based marketing will become more prevalent, say many experts, but also will become increasingly permission-based. "I'm not convinced there is a future for viral marketing involving messages thrown out to hundreds of people in the hope someone will pass it on," says Tim Patten of marketing group HHCL Digital Solutions. "But I do believe there is value where people agree to receive messages, then -- on the strength of the value of that message -- decide to pass it on." Key to the success of these marketing efforts will be companies' willingness to participate in a true dialogue with their customers: "Too many marketers still believe when they speak consumers will listen. The enthusiasm amongst marketers for developing new ways of pushing information at consumers has not been matched by an enthusiasm to listen to what consumers say." says Mark Curtis, a partner at marketing consulting group Fjord. (Financial Times 8 Jan 2002)

http://news.ft.com/news/industries/internet&e-commerce

Category 33.2 Spam

2002-01-14 spam unsolicited commercial bulk e-mail countermeasures lawsuits statistics growth

NewsScan

# THE SPAM WARS

There has been a 16-fold increase in the number of unsolicited commercial e-mail messages in the past two years (according to the spam-filtering company Brightmail), and little progress has been made in fighting it, although sporadic lawsuits have sometimes yielded (very) small (and often uncollectable) cash judgments against the spammers. The president of the anti-spam Junkbusters Corporation has compared such lawsuits to "mopping up an oil spill with a toothbrush." Yet some anti-spammers feel the effort is worthwhile, and Bennett Haselton, who recently won four judgments of \$500 each in Washington state, plans to publish a how-to guide for the spam-perplexed, hoping that if [more] people "get in the habit of taking legal action if they get spammed, then it's going to become so expensive that spammers have to get out of business." (AP/San Jose Mercury News 14 Jan 2002)

http://www.siliconvalley.com/docs/news/svfront/031444.htm

Category 33.2 Spam

2002-02-12 spam unsolicited commercial e-mail chain letter Ponzi scheme pyramid fraud

settlement government regulators

#### NewsScan

### FTC's FIGHT AGAINST SPAM

Saying that the Federal Trade Commission is "going after deceptive spam and the people who send it. We want it off the Net," FTC chairman Timothy Muris has announced that the agency has settled charges against seven people who ran an e-mail chain letter promising returns of up to \$46,000 on an investment of only \$5. The letter received responses from more than 2,000 people in nearly 60 countries. The research firm Jupiter Media Metrix says that Internet users received on the average 571 pieces of mail last year generated by unsolicited commercial mass-mailings of everything from pornography to fake diplomas; the firm predicts that number is likely to rise to 1,500 a year by 2006. (Reuters/USA Today 12 Feb 2002) http://www.usatoday.com/life/cyber/tech/2002/02/12/ftc-spam.htm

Category 33.2 Spam

2002-03-11 spam opt-in opt-out lies fraud falsehood address harvesting

RISKS 21 94ff

Discussion in RISKS erupted over a familiar scam from spammers: claiming that they are offering opt-in lists (invitations to join, permission to send) when in fact their unwanted messages reveal that they will take absence of response as tacit approval of continued spamming. The danger in replying is that since the spammers are evidently liars, they are probably lying about the results of using their opt-out e-mail addresses and so one's address is likely to be sold to yet another spammer as being validated.

Category 33.2 Spam

2002-04-22 spam costs study research industry information warfare

NewsScan

#### JUNK MAIL FALL-OUT

The founder of the anti-spam SpamCon Foundation says that "spam is a theft of both my time and my money," and industry research groups bear him out: Ferris Research has concluded that the time lost to the task of deleting spam costs about \$200 per in-box a year (and destined to go higher), and a Gartner Group study found that Internet service providers lose \$1 million for every 7 million of its members, largely because spam drives customers away. Does the future look brighter for haters of unsolicited commercial e-mail messages? Not likely. The head of the anti-spam organization Spamcop.net says: "It's an arms race. Once you close down an avenue for the spammer, he just has more of an incentive to find new ones." (San Jose Mercury News 20 Apr 2002)

http://www.siliconvalley.com/mld/siliconvalley/3108519.htm

Category 33.2 Spam

2002-07-05 spam junk phone calls cellular mobile costs consumers direct marketing

NewsScan

#### NUMBER OF JUNK CELL PHONE CALLS INCREASING

Cell phones, with their numbers unlisted, have generally been shielded from telemarketers, but that shield is becoming less effective, and an increasing number of junk calls are reaching -- and angering -- cell phone users on vacation, in their cars, or in other places they don't want to take unwanted calls (let alone have to pay for them). Companies, consumer groups, and even the Direct Marketing Association have all recognized the growing problem, and state and federal legislators are trying to deal with it through legislation. Consumer advocate Robert Biggerstaff expresses his indignation in these words: "If you eat up my minutes of cell time, you're forcing me to subsidize your advertising." (New York Times 5 Jul 2002) http://partners.nytimes.com/2002/07/05/business/05JUNK

Category 33.2 Spam

2002-09-09 spam wireless LAN local area networks ISP Internet service provides wardriving

hijacking penetration

### NewsScan

#### DRIVE-BY SPAM ATTACKS HIT WIRELESS LANs

The proliferation of unsecured corporate wireless networks is fueling a surge in drive-by spamming, a security expert warned attendees of the First International Security Users Conference in London. "These people simply drive up to a building armed with their pornographic e-mail, log into the insecure wireless network, send the message to 10 million e-mail addresses and then just drive away," said Adrian Wright, managing director of Secoda Risk Management. With more ISPs instituting no-spamming rules, these unsecured networks have become easy targets for would-be spammers. All they have to do is find an unprotected SMTP (simple mail transfer protocol) port on a company's server and then pose as legitimate users of the network -- the mail server can't tell the difference. Wright warned that between 60% and 80% of corporate wireless networks are unsecured, often because managers fail to change default settings when they install a wireless LAN. The security hole has led to the new phenomenon of "wardriving" -- driving around a city until you find an unsecured wireless LAN -- which leads to "warchalking" -- drawing a symbol in chalk on a wall or pavement to mark the presence of a wireless networking node. And the practice isn't just confined to metro areas, said Wright, producing a photo of a warchalking symbol drawn on a buoy floating at sea. (CNet News.com 6 Sep 2002)

http://news.com.com/2100-1033-956911.html?tag=fd\_top

Category 33.2 Spam

2002-11-14 spam chat rooms study test investigation

NewsScan

# THE PRICE OF CHATTING MAY BE GETTING SPAMMED

A new study by the Federal Trade Commission and other federal agencies and northeastern states has found that your participation in chat rooms will substantially increase the possibility that your name will be captured by spammers to send you junk e-mail. Surprisingly, online dating services and resume services were found to be relatively safe from spammers [but not necessarily from bad experiences, we suppose]. In an undercover operation, all the e-mail addresses planted on 250 new accounts used in chat rooms began to receive spam messages. Close behind were newsgroups [not NewsScan, which is not a newsgroup], which generated junk mail for 86% of the undercover e-mail accounts. (USA Today 14 Nov 2002) http://www.usatoday.com/tech/news/2002-11-13-spam-study

# 33.3 Antispam

Category 33.3 Antispam

2002-01-10 spam filters false positives reliability program design bounce

RISKS 21 84ff

In January 2002, AOL's spam filters rejected Harvard University's admissions-department e-mail. In the absence of any information from AOL (policy precludes their revealing any explanation of their anti-spam policies) analysts speculated that simply sending large numbers of similar messages to AOL members was enough to trigger false-positives in the filters. In discussion on the RISKS Forum, correspondents pointed out that e-mail reliability is still nowhere near that of the U.S. Postal Service. The problem was exacerbated by the lack of a bounce message to the originators; thus neither sender nor recipient could be expected to know that the messages had been discarded. Some commentators snidely suggested that using AOL as an e-mail service might be a legitimate basis for rejecting applicants. . . .

Category 33.3 Antispam

2002-01-24 antispam excess algorithm wrong bad error false positive reject verification

RISKS 21 89

Jonathan Kamens reported his frustration at trying to reach another RISKS contributor whose Internet service provider blocked his e-mail for spurious reasons. It happened that Mr Kamens was unable to send his e-mail through his usual DSL line, so he sent his message via his ISP's SMTP server. The intended recipient's mail server rejected the message because, as Mr Kamens explained it, "... this site's system administrators have decided to block all E-mail for which the host name in the envelope address can't be matched up obviously (using a simple string comparison) with the host name of the mail server sending the message. In other words, if you have your own domain name, but you send E-mail through your ISP's mail server, you simply can't send E-mail to this site."

When he tried again, this time via his restored DSL service, his mail was rejected because his mail server was incorrectly labeled as a spam relay.

Although the site claimed that they would correct mistaken assignments to the rejection list, Mr Kamens found it particularly irritating that the administrators of this picky site did not provide any way to reach them online. [MK adds that presumably, even if they had, the explanation or complaint would never make it to their e-mail inbox if it came from the affected mail server.]

Category 33.3 Antispam

2002-03-12 spam fraud abuse regulators legal action court proceeding injuction DNS Domain Name System

NewsScan

#### FTC CRACKS DOWN ON SPAM

A U.S. District Court, acting at the request of the Federal Trade Commission, has closed down the U.S.-registered Web sites of three U.K.-based companies of sending unsolicited commercial e-mail message (or "spam") to sell about \$1 million worth of phony Web addresses such as ".usa," ".sex," and ".store" for \$59 each. The Web sites closed were called www.dotusa.com, www.dotsex.com, and www.dotstore.com. The defendants say they are denying the allegations and are appealing the ruling. An FTC official says: "These scammers conned consumers in two ways. They sent deceptive spam, and they sold worthless Web addresses from their Web sites. By closing down this operation we're sending a strong signal: We will not tolerate deceptive spam." (New York Times 12 Mar 2002)

http://partners.nytimes.com/2002/03/12/technology/12SPAM.html

Category 33.3 Antispam

2002-03-22 anti-spam blackhole blacklists administration policies defaults

RISKS 22 01

Eric Murray reported in RISKS on some of the dangers of sloppy administration of anti-spam blacklists that interfered with legitimate mailings from his site. In one case, a blacklist operator chose to include an enormous block of IP addresses because one ISP was refusing to deal with one spammer; his response to complaints was, "Too bad for you, you should move." In the second case, recipients were running software that checked a whitelist of approved sources; when that list was shut down, the software received no confirmations on its checks of originating addresses and cheerfully blocked everything -- but everything -- coming into its clutches.

Category 33.3 Antispam

2002-04-10 P2P peer-to-peer AI artificial intelligence anti-spam filter e-mail signature content

inspection

NewsScan

#### INTELLIGENT SPAM FILTER

A new spam-filtering technology code-named Folsom uses a combination of peer-to-peer communications and machine learning to intercept nearly all unwanted e-mail, according to its creators. The peer-to-peer part of the technology enables a user to identify a message as spam mail, which the program then assigns a "signature" based on its content. The signatures are sent to one of numerous distributed servers where they're automatically downloaded by other members of the network and used to block copies of the same message. The machine learning part of the equation targets new spam by looking at the words and phrases in previously identified spam messages and making a judgment about the new mail. The developers say in tests of e-mail streams containing 40% to 60% spam mail, Folsom managed to reduce the percentage to "near zero" with very few "false positives." "It's a very interesting concept," says a spokesman for the Coalition Against Unsolicited Commercial Email. "Spam is getting worse, both in terms of raw volume and percentage." (New Scientist 9 Apr 2002) http://www.newscientist.com/news/news.jsp?id=ns99992141

Category 33.3 Antispam

2002-04-22 biometric identification authentication I&A access control

Security Wire Digest 4 31

# SAFLINK INTRODUCES SAFSOLUTION FOR WINDOWS

SAFLINK, a developer and integrator of biometric security solutions, last week released SAFsolution: Windows Workstation, a software product designed to replace text-based passwords with biometric authentication. The software is designed to work with a wide variety of biometric hardware: voice, face, and iris recognition devices, as well as fingerprint scanners. http://www.saflink.com

Category 33.3 Antispam

2002-05-22 spam filters content filtering research

RISKS 22 08ff

Peter G. Neumann noted that the RISKS Forum reached 98% spam content in its inbasket during a 10-day period with over 1,000 messages received. He installed SpamAssassin and the rate fell to near zero. Unfortunately, false positives continue in this field, and his announcement about spam was itself rejected by a number of spam filters because it included the trigger phrase "-n-e h-u-n-d-r-e-d p-e-r-c-e-n-t g-u-a-r-a-n-t-e-e-d" which had to be hyphenated in the followup to avoid triggering the same filters.

Category 33.3 Antispam

2002-05-22 spam content filtering blunder quality assurance QA

NewsScan

#### AT&T's FILTER FILTERS AT&T's MAIL

An example of foot-in-mouth filtering? AT&T Broadband offered its high-speed Internet users an e-mail software filter to block spam, but later found out that it had blocked its own messages to customers notifying them of a rate increase. An AT&T executive tried to put the best face on it: "If there is a silver lining, it appears our spam filtering system works so well that it even deletes mass e-mails from our own company." The company will resend customer notices of the rate increases. (AP/USA Today 2002)

http://www.usatoday.com/life/cyber/tech/2002/05/22/e-mail-filter.htm

Category 33.3 Antispam

2002-05-29 anti-spam legislation Europe cookies privacy surveillance controls legislation

proposals law

NewsScan

#### EUROPEAN PARLIAMENT CLOSE TO SPAM BAN

A bill that would outlaw unsolicited commercial e-mail and prohibit the unauthorized placement of files (such as cookies) on people's computers is close to passage in the European Parliament. In a nod to heightened concerns over cybercrime and terrorist activities, the bill would also give European law enforcement officials greater access to electronic records of people's phone calls and Web visits by allowing the retention of such records "for a limited period" to safeguard national security and aid the "prevention, investigation, detection and prosecution of criminal offenses." The proposed legislation is the result of two years of intense lobbying by consumer groups, e-commerce firms, law-enforcement officials and privacy advocates. "We'll get a good and delicate balance between the needs of law-enforcement agencies and the respect of human rights," says a spokesman for the European Commission. (Wall Street Journal 29 May 2002)

http://online.wsj.com/article/0,,SB1022615363371120040.djm,00.html (sub req'd)

Category 33.3 Antispam

2002-08-22 junk fax federal regulators fine fraud deception lawsuit

NewsScan

#### JUNK FAXES

The Federal Communications Commission wants to levy a \$5.4 million fine on Fax.com, a company that uses a fax-number database to distribute faxed ads for its customers (restaurants, auto repair shops, and so forth). The FCC said that Fax.com has "engaged in a pattern of deception to conceal its involvement in sending the prohibited faxes," which has been banned since the passage of the Telephone Consumer Protection Act of 1991. Fax.com's attorney, Mary Ann Wymore, regards the ban as "a clear infringement on commercial speech rights," and predicts it ultimately will be overturned by the U.S. Supreme Court. (Wall Street Journal 8 Aug 2002)

#### MAD AS HELL OVER JUNK FAXES

Steve Kirsch, a Silicon Valley entrepreneur and philanthropist, is suing the fax-broadcasting company Fax.com for \$500 billion (repeat: billion) in statutory damages, assuring skeptics: "This is not a publicity stunt; our goal is to shut Fax.com down and make any advertiser thinking of sending an unsolicited fax think twice... I have the resources, time and money." (San Jose Mercury News 22 Aug 2002)

Category 33.3 Antispam

2002-09-24 spam text messaging cell phones legislation law bill

NewsScan

# BAN ON CALIFORNIA SPAMMIN'

A new California law that will take effect in January bans the unsolicited sending of text messages to cell phones. The bill's author, Assemblyman Tim Leslie (R, Tahoe City), says the bill is intended to stop spam text messages from getting as out of control as spam e-mail messages. The bill is part of a package (called "leave-us-alone-legislation), which also bans unsolicited fax ads and which makes changes to California's "do-not-call" list for telemarketers. (AP/USA Today 23 Sep 2002)

Category 33.3 Antispam

2002-09-27 spam buld e-mail junk lawsuit government law

NewsScan

#### CALIFORNIA SUES BULK MAILER

Under a four-year-old anti-spam law that has had little success in controlling unsolicited bulk commercial mail ("spam") over the Internet, California's attorney general has filed a \$2 million lawsuit against the PW Marketing Group for sending millions of spam messages, and for failing to include in their messages a valid return address, as required by the law. Calls to PW Marketing have not been returned. To explain the failure to produce more successes over the four years in which the law has been in effect, a spokesperson for Bill Lockyer, the California attorney general, says that anti-spam lawsuits are "difficult, complex cases, and time-consuming." (San Jose Mercury News 26 Sep 2002)

Category 33.3 Antispam

2002-10-21 spam cellular phones wireless law legal restrictions database

NewsScan

#### ENDING MARKETING CALLS TO CELL PHONES

To help telemarketers comply with a 1991 federal law banning auto-dialed or prerecorded commercial calls to cell phones, the Direct Marketing Association has identified 280 million existing and prospective wireless numbers for its member businesses to avoid calling. Member companies have been afraid they'll get into trouble for inadvertently calling cell phone numbers not readily distinguishable cellular from landline numbers. (New York Times 21 Oct 2002)

Category 33.3 Antispam

2002-10-30 spammer court legal action settlement ban bulk junk e-mail

NewsScan

#### VERIZON SILENCES SUPER-SPAMMER

Verizon has reached a legal settlement that bans Alan Ralsky, whose company Additional Benefits LLC is considered to be one of the world's largest sources of bulk e-mail, from sending messages to its 1.64 million Internet access customers. Verizon had filed its lawsuit against Ralsky in March 2001 after several incidents in which Verizon customers were inundated with millions of e-mail solicitations for online casinos, diet pills, credit repair services, etc. The complaint said Ralsky broke federal and Virginia laws by, among other things, clogging its network with illegitimate e-mails. Ralsky must also pay an undisclosed fine, but apparently remains unfazed the recent action, stating that he has lists of 150 million e-mail addresses, so the Verizon case will eliminate only a small portion of those. (AP 30 Oct 2002)

http://apnews.excite.com/article/20021030/D7MVTD300.htm

Category 33.3 Antispam

2002-11-12 anti-spam e-mail address change consumers costs marketing businesses

NewsScan

#### E-MAIL ADDRESS CHURN GIVES E-TAILERS HEARTBURN

Almost a third of U.S. Internet users change their e-mail addresses each year, costing businesses millions in potential sales, according to a new study by NFO WorldGroup. Reasons cited for changing e-mail addresses include changing jobs, switching ISPs, or evading spam. Recently, 87% of total respondents had changed a personal e-mail address and 35% had changed a work address. At least 16% said the change was intended specifically to shake off spammers whose tactics have become increasingly aggressive and subject matter increasingly offensive. The high turnover rate has caused headaches for legitimate businesses, however, who lose contact with customers who may have volunteered their e-mail addresses as part of the business relationship. "It's too much of a hassle to update their personal information with the sites," says an NFO marketing manager. "They look at it and think if they have to go through this process with 20 Web sites, it's too much trouble. Whereas with contacting 20 friends, that's a different thing." Return Path, an e-mail change-of-address company, estimates that e-mail churn cost businesses between \$3 billion and \$4 billion in 2000 due to lost sales, wasted e-mail acquisition marketing and unnecessary e-mail delivery costs, with those losses rising to \$10 billion to \$20 billion in five years. (Wired.com 12 Nov 2002) http://www.wired.com/news/business/0,1367,56049,00.html

Category 33.3 Antispam

2002-11-27 anti-spam research archive database filters fight battle

NewsScan

#### SPAM ARCHIVE PROJECT SEEKS CONTRIBUTIONS

CipherTrust wants your spam, including every e-mail come-on for Viagra, "free" pornography, and adult services. But they aren't masochists -- they're hoping to build an archive of spam (www.spamarchive.org) that programmers and researchers can use in the never-ending fight against unsolicited e-mail. The company hopes to collect at least 10 million spam samples within a year, and is already well on its way to meeting its goal. "This should eliminate one of the big bottlenecks for people who want to make anti-spam tools," says one programmer who has developed mail-filtering programs. "You can write all the code you want, but it won't do a whole lot of good unless you have a large amount of spam to test your algorithms on." CipherTrust says it will use the archive to help its technicians improve "IronMail," its proprietary anti-spam product. Still, even the best junk e-mail filters won't stop determined spammers, says programmer and open source enthusiast Eric Raymond: "It's like a whack-a-mole game: you shut down (spam e-mail) servers in one place, and the same spammers pop up again in another place running a shoestring operation out of their basement. But in a weird way, that sort of highlights one of the Internet's strengths, that it's very hard to lock someone out of communication or suppress speech." (Washington Post 26 Nov 2002)

# 34.1 Net filters

Category 34.1 Net filters

2002-01-23 censorware content filtering antispam algorithm simplistic false positive availability

RISKS 21 90

MS-Outlook's "adult content filter" assumes that the phrase "over 18" automatically and inevitably means that an e-mail message is pornographic spam. Outlook therefore rejected an issue of Microsoft's own e-mail MSDN Flash newsletter because it contained the phrase "provides over[space]180 hours of content in three technical conferences."

Category 34.1 Net filters

2002-04-11 intellectual property law proposals censorship censorware libraries content filtering

RISKS 22 03

Marc Rotenberg published a thoughtful essay in RISKS celebrating the 50th anniversary of the publication of Ray Bradbury's novel, \_Fahrenheit 451\_, drawing parallels between the nightmarish world of the novel and some of the trends he sees in the USA today. In the novel, all written language is banned; in today's America, "Already software filters have been turned on controversial ideas and unpopular organizations. And new copyright techniques will digitally incinerate recorded words that might otherwise be widely available."

Category 34.1 Net filters

2002-12-11 content filtering pornography study research libraries

NewsScan

#### A LITTLE BIT OF ANTI-PORN FILTERING CAN GO A LONG WAY

"A little bit of filtering is O.K., but more isn't necessarily better," says Vicky Rideout, vice president of the Henry J. Kaiser Family Foundation, which conducted a study showing that when anti-pornography Internet filtering software is set at a low level of restriction, it's just as effective as when it is set a high level, and is far less likely to prevent searchers from reaching bona fide health sites. But some observers, such as Judith F. Krug of the American Library Association, think that filters are such blunt instruments that they should not be used at all in public institutions: "Filters are just fine for parents to use at home. They are not appropriate for institutions that might be the only place where kids can get this information." The filtering programs generally block any references to sex-related terms; examples given by the report include such subjects as safe sex, condoms, abortion, jock itch, gay, and lesbian. (New York Times 11 Dec 2002)

# 34.2 Usage monitoring, audit trails (employees, children)

Category 34.2 Usage monitoring, audit trails (employees, children)

2002-02-17 surveillance technology spyware logging audit trail employee privacy keystroke

logging pornography appropriate use policy

#### NewsScan

#### THE CASE OF THE HORRIFIED SPY

The man who conceived and wrote the software thinks of himself as a privacy lover and says that what his program does is "horrifying": "Every time I add a feature into it, usually it's something that I've fought for a long time." But he's sold more than 200,000 copies of his \$99 downloadable Investigator software, which can read every e-mail message, instant message and document someone sends and receives, and will take pictures from a Web cam, save screen shots, and read keystrokes in numerous languages. The program is hidden on the target's computer, as are the files containing the information it gathers. Ari Schwartz of the Center for Democracy and Technology concedes that the surveillance technology is a valuable tool in fighting fraud or child pornography, but thinks that companies need to resist using it too readily because "we think morally there are some very large issues" raised when employers track the personal habits of their workers. (AP/San Jose Mercury News 17 Feb 2002)

http://www.siliconvalley.com/mld/siliconvalley/2693278.htm

Category 34.2 Usage monitoring, audit trails (employees, children)

2002-04-12 privacy monitoring corporate policy instant messaging

NewsScan

#### COMPANIES START TRACKING WORKERS' INSTANT MESSAGES

Employees have known for several years that their bosses are keeping an eye on their telephone and e-mail habits, but new technology now makes it possible to monitor instant messaging exchanges as well. Privacy advocates say they know of no major instances where employees have been disciplined for IM abuse, but that it's probably just a matter of time. As of last year, only 20% of all IM accounts belonged to business users, but that percentage is expected to rise to 50% by 2004, according to the Radicati Group. Meanwhile, some companies have reported more diligent workers after they installed e-mail monitoring software on their corporate systems. "It changed the employee behavior. Their productivity went up," says one marketing director. "They were a little bit more careful with their communication. It will be the same with IM," she predicts. (AP 12 Apr 2002)

http://apnews.excite.com/article/20020412/D7IRHP780.html

Category 34.2 Usage monitoring, audit trails (employees, children)

2002-12-10 surfer content filtering work appropriate use wasting time

NewsScan

### SURFERS: WHAT COULD THEY BE THINKING?

A study by Aaron Schatz has found that the top ten search terms used on Lycos Net this year have been: 1, Dragonball (the Japanese cartoon); 2, Kazaa (the music and video file-swapping service); 3, tattoos (that's right -- tattoos); 4, Britney Spears, the pop singer who, oops, did it again; 5, Morpheus (file-swapping); 6, NFL, the National Football League; 7, IRS; 8, Halloween; 9, Christmas; and 10, Pamela Anderson, the actress and, uh, celebrity icon. Schatz says, "No matter how the news ebbs and flows, people still use the Internet for entertainment." So we see. There just doesn't appear to be that big a demand for information on the origins of the First World War. (USA Today 10 Dec 2002)

# 35.1 Cybersquatting

Category 35.1 Cybersquatting

2002-02-15 cybersquatting dishonesty Web hijacking political propaganda trickery

NewsScan

#### LYING FOR TRUTH

Some unknown person or group has created a Web site called www.reedcollegis.com intended to fool people looking for Reed College (www.reed.edu) and send them an anti-abortion site called www.abortionismurder.com. Reed College chief technology officer Martin H. Ringle says, "We've paid for 'reed.com' and 'reed.org,' and so on, in an effort to pre-empt cybersquatting. But it's impossible to imagine every variation of the name and how it could be used -- although in hindsight, reedcollegis.com was an obvious one." The site abortionismurder.com is maintained by a Florida man, Thomas P.A. Fitch, who denies involvement with or knowledge of the creation of reedcollegis.com, but does admit to owning an address similar to that of the College Board. His aim is to attract college applicants to his anti-abortion site to expose "to the truth" students who are "going to run this country in fifteen years... I'd say our tactics are not dishonest. They're creative, they're on the edge, they're bold. Thank you for the publicity because it's only helping our cause." Sheldon E. Steinbach of the American Council on Education says of use of the name reedcollegis.com to divert unsuspecting surfers from their intended goal: "This is the first instance, to my knowledge, that a university or college name has been hijacked for seemingly a political purpose." (Chronicle of Higher Education 15 Feb 2002)

http://chronicle.com/free/2002/02/2002021501t.htm

Category 35.1 Cybersquatting

2002-05-27 DNS Domain Name System hijacking pornography

RISKS 22 10ff

Geoffrey Bent noted in RISKS:

When the US Navy forgot to renew registration on NavyDallas.com - apparently because Network Solutions forgot to send them a renewal notice - it was snapped up by a pornography site. NSI accepted the new registration despite the new owner being identified simply as "Bog". Meanwhile, NavyBoston.com now directs users to an eBay auction site:

http://www.newsbytes.com/news/02/176741.html

Category 35.1 Cybersquatting

2002-06-27 cybersquatting intellectual property extortion domain name system DNS Domain Name System pornography gambling rules dispute registration

NewsScan

#### ICANN PROPOSES RULES TO FIGHT CYBERSQUATTING

The Internet Corporation for Assigned Names and Numbers (ICANN) says it's close to adopting new procedures that would make it easier for individuals and businesses to avoid extortion by cybersquatters, and would establish a waiting list for coveted domains that become newly available to the public. The first measure would establish a 30-day grace period for domain name owners to renew their contracts -- a move intended to prevent speculators from swooping in and registering an expiring domain name before the owner has time to renew. "ICANN receives a large number of complaints for inadvertently deleted domains It affects churches, schools, businesses," says an ICANN spokesman. "We get a lot of complaints from people who wake up to find their domain has expired and now has porn on it, or it's linked to a casino site. Then, they'll ask for a ransom to get it back." The waiting-list proposal would allow a bidder to pay a fee to get first dibs on any newly available domain names. That proposal has run into opposition from registrars who say the \$28 that VeriSign has proposed charging them for the service is too high. (Reuters/Wired 27 Jun 2002)

http://www.wired.com/news/politics/0,1283,53518,00.html

Category 35.1 Cybersquatting

2002-07-30 cybersquatting DNS Domain Name System conflicts extortion

NewsScan

# WHAT WAS A DOT-COM LAND GRAB, DADDY?

Cybersquatting is virtually (no pun intended) a thing of the past -- and cyber "real estate" is definitely losing value. The number of dot-com, dot-net, and dot-org names has declined by more than 11% in the first five months of this year, and industry analysts are saying that the dot-com land grab is over. This is quite a change from those heady days, not so long ago, when desirable dot-com names could fetch hundreds of thousands of dollars from companies eager to project just the right image to customers. Now, companies like Johnson & Johnson are saying: "It's become clear that we've already registered as many domain names to protect our trademarks as we need. We haven't needed to buy any more this year." So what will cybersquatters do now? One knowledgeable observer of the scene says, "Speculation is gone. The days of hunting out a real business opportunity are here." Maybe the cybersquatters will actually get a real job. That would be nice. (Los Angeles Times 29 Jul 2002)

# 35.2 Trademarks vs DNS

Category 35.2 Trademarks vs DNS

2002-01-16 DNS domain name system registrar trademark conflict investigation

NewsScan

#### INTERNET REGISTRAR CHALLENGES '.INFO' TRADEMARK CLAIMS [16 Jan 2002]

Afilias, the company responsible for registering ".info" names, is challenging 741 registrations made by people who claimed they owned the trademark on the name. Afilias says it didn't have the time to verify that applicants actually held the trademarks that they claimed. "It would have been too complicated and slow, since there is no unified worldwide database for trademarks," says Phillipp Grabensee, an Afilias board member. "We would have had to check every single brand." Afilias is now attempting to sort through its database and weed out fraudulent applications, referring them directly to an international mediator for resolution. During the two-month period set aside for trademark holders to preregister for their names, 52,245 names were registered, and it's estimated about 20% of those names were fraudulently acquired. "Some people seem to have registered a whole dictionary," says Grabensee. (Handelsblatt/Wall Street Journal 16 Jan 2002) http://interactive.wsj.com/articles/SB10112144497968880.htm (sub req'd)

Category 35.2 Trademarks vs DNS

2002-08-23 cybersquatting Domain Name System DNS conflict lawsuit settlement

NewsScan

#### FORD MOTOR COMPANY SETTLES DISPUTE OVER 'FORDFIELD' DOMAIN NAME

Ford Motor Company has settled its federal lawsuit against, Michael Ouellette, the owner of a T-shirt and grass seed business named Ford Field Inc., which the entrepreneur had registered on the Internet as "fordfield." Ford had charged Ouellette with trademark infringement and cybersquatting, but he insisted that his inspiration for the name had been a public baseball diamond where he used to play ball. (AP/New York Times 22 Aug 2002)

# 35.3 Politics of the DNS

Category 35.3 Politics of the DNS

2002-01-21 DNS domain name system lottery

NewsScan

#### REGISTRARS REJECT VERISIGN'S 'PAY-TO-WAIT' PROPOSAL [21 Jan 2002]

Internet domain name registrars overwhelmingly oppose VeriSign's proposal to create a pricey waiting list for registered domain names, calling it too expensive and anti-competitive. VeriSign has suggested charging registrars \$40 for first dibs on a registered domain name. A subscriber would be guaranteed first-refusal rights to the name if it becomes available, but would still have to pay even if the current owner decided to renew its subscription. VeriSign said the waiting list would provide a new source of revenue and discourage speculation in domain names by raising the cost. Other registrars complained that instead of solving the cybersquatting problem, the proposal would just shift the action to the waiting list. In addition, some expressed suspicions that VeriSign would use the waiting list to hoard all the best names for itself, but Chuck Gomes, VP of policy and compliance for VeriSign's Global Registry Services, said his company maintained a strict "firewall" between the two sides of the business: "I ensure that day by day we're not advantaging any registrar I understand the mistrust, but it's unwarranted." (Wired.com 21 Jan 2002)

http://www.wired.com/news/business/0,1367,49756,00.html

Category 35.3 Politics of the DNS

2002-02-25 DNS domain name system government involvement politics policy model

NewsScan

#### ICANN PRESIDENT WANTS MORE GOVERNMENTAL PARTICIPATION

Stuart Lynn, president of the nonprofit Internet Corporation for Assigned Names and Numbers, says the organization he heads needs to be restructured to obtain more governmental participation: "I am now convinced that the original desire to avoid a totally governmental takeover ... led to an overreaction -- the choice of a totally private model." Such a model is unworkable, Lynn says, because it leaves ICANN "isolated from the real-world institutions -- governments -- whose backing and support are essential." His recommendation calls for the next ICANN board to have 15 members -- one-third nominated by governments, one-third selected through a committee process, and the remaining consisting of the group's president and appointments by four policy and technical groups. (AP/San Jose Mercury News 25 Feb 2002) http://www.siliconvalley.com/mld/siliconvalley/2741326.htm

# NEW PROPOSAL DISPARAGED BY ICANN CRITICS [25 Feb 2002]

The proposal made by ICANN president Stuart Lynn to expand the participation of the world's governments in making policy decisions over Internet domain names and other issues is being widely criticized for "closing the door to the public" (Karl Auerbach) and for giving "totalitarian governments power to influence rules that would go into direct effect in the United States" (Michael Froomkin). Lynn maintains that the national governments are "the most evolved form of representation of the public interest," even if not all are democratic. The acronym ICANN stands for Internet Corporation for Assigned Names and Numbers. (AP/San Jose Mercury News 25 Feb 2002)

http://www.siliconvalley.com/mld/siliconvalley/2745051.htm

Category 35.3 Politics of the DNS

2002-03-15 **DNS** domain name system governance

NewsScan

# ICANN REJECTS BOARD MEMBER ELECTIONS

ICANN, the international nonprofit group that sets policy for the Internet's "domain-naming" (i.e., addressing) system, has decided against electing its board members by general elections, at least for the time being. In an ICANN meeting in Ghana, board chairman Vinton Cerf said, "It is obvious to all of us after carefully examining the issues that we're not doing elections now" -- and ICANN chief executive Stuart Lynn said the reason for the decision was that most board members feared general elections could be marred by fraud and dominated by special interests. Board member Karl Auerbach dissented vehemently from the group's decision: "ICANN made a great leap backwards. It repudiated the compact on which it was formed -- an agreement that ICANN would, being a public and tax-exempt entity, allow the public to meaningfully participate." The acronym ICANN stands for the Internet Corporation for Assigned Names and Numbers. (AP/San Jose Mercury News 14 Mar 2002)

http://www.siliconvallev.com/mld/siliconvalley/2861182.htm

Category 35.3 Politics of the DNS

2002-03-20 DNS Domain Name System governance lawsuit

NewsScan

#### ICANN SUED BY ONE OF ITS BOARD MEMBERS

ICANN dissident board member Karl Auerbach is suing to gain access to the group's travel records, payroll figures, and other information he says he needs "to exercise independent judgment and fulfill my duties as director." ICANN staff have refused to provide him that kind of information unless he first signs a confidentiality agreement, but he has attacked them for being secretive and unaccountable to millions of Internet members. In his lawsuit, Auerbach is being represented by the civillibertarian Electronic Frontier Foundation. (Reuters/USA Today 18 Mar 2002)

http://www.usatoday.com/life/cyber/tech/2002/03/18/icann-sued.htm

Category 35.3 Politics of the DNS

2002-04-01 DNS Domain Name System governance

NewsScan

#### CRITICS TELL ICANN: NO YOU CAN'T

Critics of the nonprofit organization ICANN (the Internet Corporation for Assigned Names and Numbers) continue to be unimpressed with efforts (or perceived lack thereof) to involve ordinary Internet users in the process of managing the Internet. Criticized for his recent proposal to revamp the organization's board and committee structure, ICANN president and chief executive M. Stuart Lynn says, "The proposal put on the table was bound to change. If there are better ways, let's hear them." See www.icann.org. (New York Times 1 Apr 2002)

http://www.nytimes.com/2002/04/01/technology/ebusiness/01DOMA.html

Politics of the DNS Category 35.3

2002-05-21 DNS Domain Name System children legislation law

FindLaw Download This 86

#### HOUSE APPROVES DOT-KIDS INTERNET DOMAIN

The House of Representatives' today approved legislation designed to cordon off a safe online "playground" for young children. House members voted 406-2 to approve the "Dot-Kids Implementation and Efficiency Act of 2002," which would mandate the creation of a "dot-kids" extension within America's sovereign "dot-us" Internet domain. The new Internet addressing space "will be a cyberspace sanctuary for content that is suitable for kids," said Rep. Edward Markey (D-Mass.) during today's debate.

http://www.newsbytes.com/news/02/176705.html

Dot-Kids Implementation and Efficiency Act of 2002 (H.R. 3833)

[Copy and paste link into browser] [PDF]

http://frwebgate.access.gpo.gov/cgibin/getdoc.cgi?dbname=107\_cong\_bills&docid=f:h3833ih.txt.pdf

Politics of the DNS Category 35.3

2002-06-11 **DNS Domain Name System governance** 

NewsScan

### DYSON SAY ICANN HAS BECOME 'A REAL CESSPOOL'

Esther Dyson, tech celeb and former chair of ICANN (the Internet Corporation for Assigned Names and Numbers), told an audience at the Wharton business school that "ICANN has become a real cesspool," because of its tangled disputes about authority, accountability, and openness. The independent agency is in charge of managing policy for the Internet's name and address systems. "When I was a young student, I thought grow-ups would come and make things work. Now I realize that grown-ups are just kids with wrinkles. I only see juvenile behavior at ICANN." (Public Policy & Management Emory, Jun 2002)

http://knowledge.emory.edu/articles.cfm?catid=9&articleid=517&homepage=yes

Category 35.3 Politics of the DNS

2002-06-13 DNS Domain Name System governance

NewsScan

#### ICANN BY ANY OTHER NAME WOULD BE THE SAME

Testifying before a Senate subcommittee showing skepticism about the performance of ICANN, the nonprofit organization set up to assign Internet names and numbers and set policies to guide the Internet, U.S. Commerce Department official Nancy Victory said that "the department continues to be supportive of the ICANN model," and suggested that establishing a new group to take its place would accomplish nothing: "Yes, it gets you a new bunch of people, yes it gets you a new company with a new name, but you still encounter the same problems." Without disagreeing with Ms. Victory, subcommittee chairman Ron Wyden (D-Ore.) said: "If ICANN is going to reform itself, the Department of Commerce is going to have to push the organization harder than they have done in the past." (Reuters/New York Times 12 Jun 2002) http://partners.nytimes.com/reuters/technology/tech-tech-icann.html

Category 35.3 Politics of the DNS

2002-06-25 DNS Domain Name System governance dispute conflict business government membership

#### NewsScan

#### SHOW-DOWN IN BUCHAREST

At its annual meeting in Bucharest this week the nonprofit organization ICANN, which stands for Internet Corporation for Assigned Names and Numbers, will be facing its fiercest critics and defending its recent proposal to limit ICANN board membership to representatives of business and government. Long-time ICANN critic and University of Miami law professor Michael Froomkin says: "I don't think governments are needed, nor at this time are they organized in a manner that would make their representation easy. The officials who turn up to ICANN meetings are the ones who heard about the Internet first, not necessarily the people who make, or should make, Internet policy." (Reuters/San Jose Mercury-News 25 Jun 2002) http://www.siliconvalley.com/mld/siliconvalley/3540508.htm

Category 35.3 Politics of the DNS

2002-09-23 DNS Domain Name System governance politics

NewsScan

#### ICANN WINS ANOTHER YEAR

The U.S. Commerce Department has given a one-year renewal to ICANN (the Internet Corporation for Assigned Names and Numbers), whose mission is to oversee the Internet's domain name system. Acknowledging some criticisms that the group is not sufficiently accountable to the public, the Commerce Department is telling ICANN to increase participation from the broader Internet community and to make the group's decision-making processes more open. (AP/San Jose Mercury News 21 Sep 2002)

Category 35.3 Politics of the DNS

2002-10-15 DNS Domain Name System politics governance

NewsScan

# INTERNET SOCIETY TO MANAGE '.ORG'

ICANN (the Internet Corporation for Assigned Names and Numbers) has tapped the nonprofit Internet Society to manage domain names ending in ".org" beginning next year. Currently, those names are managed by VeriSign Global Registry Services, whose contract expires Dec. 31, 2002. ICANN officials say the Internet Society plans to create a new nonprofit organization, dubbed the Public Interest Registry, which will subcontract with Afilias to handle the registration business. Afilias also operates the ".info" domain name. (AP 15 Oct 2002)

http://apnews.excite.com/article/20021015/D7MLV78O0.htm

Category 35.3 Politics of the DNS

2002-10-31 DNS Domain Name System governance politics

NewsScan

#### ICANN UNDER NEW ATTACKS

ICANN -- the Internet Corporation for Assigned Names and Numbers -- is one of those organizations apparently destined for continuous controversy. The organization recently eliminated five sitting board members from the 18-person directorate, leading to new charges of its running a closed and "illegitimate" organization. Hans Klein, chairman of the Computer Professionals for Social Responsibility, says of ICANN's leaders: "I think legitimacy matters, they don't. If you kill the legitimacy of an organization, you put the organization at risk. ICANN has decided that legitimacy doesn't matter; it's done away with many of the mechanisms that insured its legitimacy. If people start leaving the organization, it will be ruined." And Michael Froomkin, another ICANN critic, says: "What's outrageous is that because the ICANN staff can't stand to have its actions questioned, it's making sure it never has to face the user community in an election again. In fact, in the new 'reform' plan, ICANN's insiders have put themselves in charge of the process that will select their successors." (Internet News 30 Oct 2002)

Category 35.3 Politics of the DNS

2002-11-12 DNS Domain Name System governance

NewsScan

#### ICANN TO CREATE THREE MORE 'SPONSORED' DOMAINS

ICANN, the nonprofit Internet Corporation for Assigned Names and Numbers, is planning the creation of three new "sponsored" (or narrowly focused) Internet address domains, which, like dot-museum (for the museum community) or dot-coop (for employee-owned co-op organizations), will be reserved for specific audiences (as contrasted with, say, dot-com, which is open to all potential registrants). The reason for this strategy, says ICANN president Stuart Lynn, is to avoid a gold-rush environment that characterized the creation of new domains in the past. But ICANN board member Karl Auerbach, who is also a long-time critic of the organization, accuses Lynn of "making a down-and-out decision about who can be in business on the Internet and who cannor"; he thinks ICANN is creating an artificial scarcity of domain names, to benefit businesses that sell existing domains. (Washington Post 11 Nov 2002)

Category 35.3 Politics of the DNS

2002-12-16 domain name system DNS regulations limits trademarks

NewsScan

# ICANN HEAD FAVORS MEMBERS-ONLY DOMAINS [10 Jan 2002]

ICANN president M. Stuart Lynn says he favors creating new members-only suffixes, such as .edu and .museum, over unrestricted domains such as .biz and .info. "A lot of the problems surrounding the new (top-level domains) are less (common) in a sponsored environment," he said, echoing sentiments expressed by ICANN chairman Vint Cerf at a meeting in December. Problems such as cybersquatting disputes would be greatly diminished in a more tightly regulated domain, said Lynn. "It may be that a number of these cybersquatting or trademark disputes are going to be less because there's a lot of careful evaluation to make sure that someone really is using them for their announced" purpose. Lynn and Cerf have both emphasized that their opinions are their own and not those of ICANN, but that they've talked with many people who agree with them. "More people I talk to think it's the more likely direction," said Lynn. (Reuters/CNet 10 Jan 2002) http://news.cnet.com/news/0-1005-200-8436749.html?tag=mn\_hd

### THE INTERNET NAME GAME [14 Jan 2002]

The London-based Global Name Registry has begun offering registration of Internet names for individual persons. Name registration will cost about \$30 a year (not including Internet access), and the registry plans to expand ".name" designations to mobile phones and other personal devices by the end of the year. (AP/San Jose Mercury News 14 Jan 2002) http://www.siliconvalley.com/docs/news/svfront/002411.htm

#### ICANN ENDORSES NEW DOMAINS

At its annual meeting, ICANN (Internet Corporation for Assigned Names and Numbers) said it will endorse a limited number of new top-level domains for only the second time since 1985. The next group likely will be "sponsored domains" targeting a specific industry or field, such as .travel, .news, or .health. The decision will please some of the business that have been clamoring for ICANN to open up new addresses, but will also inevitably bring more disputes. "There will always be controversy. It's a very different world we're in today, a very noisy world," said ICANN president M. Stuart Lynn. (Wall Street Journal 16 Dec 2002)

# Education in security & ethics

Category 37 Education in security & ethics
2002-01-19 human factors error efficiency effectiveness training

RISKS 21 87

In an illustration of the importance of training for effective use of security measures, Dan Birchall reported on the introduction of speed cameras in Honolulu:

>After much debate, and general wailing and gnashing of teeth from those who like to drive fast, the powers that be here in Honolulu have a private contractor operating cameras to photograph vehicles which speed or run red lights. After the license number, time, and location of the violation are verified, a citation is mailed.

In their first day of operation, the cameras caught 927 speeders. http://starbulletin.com/2002/01/03/news/index1.html

However, more than 80% were unenforceable due to human errors in operation of the cameras - poor aim, inaccurate location recording, etc.

http://starbulletin.com/2002/01/08/news/index4.html

< .

Category 37 Education in security & ethics

2002-01-20 academic education cyberterrorism infrastructure protection homeland security

Security Wire Digest 4 5

# MORE NEEDED TO GET WORKERS, STUDENTS INTO SECURITY

Congress needs to do more to encourage students and government employees to specialize in information security if cyberterrorism laws, such as the PATRIOT Act, are to succeed, say members of a network security symposium last week. Panelists at the Computing Technology Industry Association and Infrastructure Security Dialog said better trained infosecurity personnel are needed to make recently approved anti-terrorism measures work as intended. That's prompted several bills focused on security education, including the Homeland Security Education Act introduced by Sen. Richard Durbin (D-Ill.). That proposal and a similar bill for federal workers would offer financial incentives, such as fellowships and student loan repayment, to college students and government professionals who specialize in computer security.

For more information on the Homeland Security Education Act and its companion, the Homeland Security Federal Work Force Act, go to:

http://thomas.loc.gov/cgi-bin/query/C?c107:./temp/~c107iJmMdFhttp://thomas.loc.gov/cgi-bin/query/C?c107:./temp/~c107gbgWnW

Category 37 Education in security & ethics

2002-02-07 anti-fraud online safety security privacy education awareness Web alliance

consumer protection

#### NewsScan

# NEW SUPPORT GROUP TARGETS PC SECURITY

A government-and-business alliance called the Stay Safe Online Campaign has established a site at http://www.staysafeonline.info to provide home and small business computer users with information about security techniques to protect themselves against network vandals. A spokesman for the group explains that individuals and small businesses "don't have the infrastructure support that people who work in large companies have at the office," and a recent study by Digital Marketing Services found that 97% of such users are vulnerable to attacks on the Internet because they fail to update antivirus software on a regular basis. (San Jose Mercury News 7 Feb 2002)

http://www.siliconvalley.com/mld/siliconvalley/2627667.htm

Category 37 Education in security & ethics

2002-02-14 Internet fraud scam teenagers adolescents children ethics training education law

enforcement police prevention prediction

NewsScan

#### INTERNET KIDS: I WAS A TEENAGE SCAMMER

FBI agent Frank Harrill of the Los Angeles cybercrime squad says, "We have seen a rise in the crimes [Internet scams], with an increasing degree of sophistication by a younger demographic. I think it's safe to say we are going to see more of it." The use of the Internet to make fraudulent credit card purchases with stolen account numbers has become a fairly common practice. One knowledgeable observer says, "It's easy for them to pull off. A lot of teens don't take it seriously. They think it's a game." Chris Painter of the U.S. Department of Justice thinks he sees an answer to the problem: "We have to teach these kids some kind of cyberethics." (AP/USA 14 Feb 2002)

http://www.usatoday.com/life/cyber/tech/2002/02/14/net-scammers.htm

Category 37 Education in security & ethics

2002-04-22 malware online discussion group education certification

RISKS 22 04

Rob Slade announced a new group:

>I have created a Yahoo group for the Anti-virus Management and Protection topic, notified the CASPR people, and have apparently been accepted as the group leader. I have used the name malware in order to be somewhat more inclusive in the discussion. (I note that in CASPR viruses come under Computer Operations, whereas they appear in Applications Development in the ISC2 domains.)

The group name is CASPRmalware. To join, send e-mail to: CASPRmalware-mailto:subscribe@yahoogroups.com or see the group home page:

http://groups.yahoo.com/group/CASPRmalware

The group e-mail address is: mailto:CASPRmalware@yahoogroups.com

This group is for discussion and preparation of the CASPR (Commonly Accepted Security Practices and Recommendations, http://www.caspr.org), Anti-virus Management and Protection document.<

Category 37 Education in security & ethics

2002-04-25 university education academia security research policies scholarship

Security Wire Digest 4 32

# \*COLLEGES ASKED TO MAKE CYBERSECURITY BIGGER PRIORITY

Colleges are being asked to pledge their support for better cybersecurity by making IT security a bigger priority on campus. "It's not just about protecting research going on at your (university). It's about protecting your country," said cybersecurity czar Richard Clarke last week at an IT conference focused on higher education. Clarke asked university administrators to endorse a framework that calls for more research in information security and better collaboration with government agencies. It also asks colleges and universities to better defend their own networks against attacks. The pledge request comes seven months after the National Science Foundation launched a federal scholarship program at 10 universities to encourage students to study information security. Every year of financial support must be repaid with a year of employment with the federal government.

Category 37 Education in security & ethics 2002-06-06 security awareness posters

Security Wire Digest 4 44

# \* NSA LAUCHES CYBER "SECRECY" CAMPAIGN

Powerful images of soldiers and sailors towering over the banner "Information Security Begins with You" are the cornerstone of a new National Security Agency campaign to raise infosec awareness in military ranks. With poster reminiscent of the World War II era "Loose Lips Sinks Ships" campaign, the NSA hopes the awareness program will make military personal more cognizant of the importance of preventing information--including electronic data--from reaching the hands of terrorists and foreign adversaries in the post-9/11world. "We hope to increase the awareness of military personnel to the absolute necessity of guarding sensitive information, using secure communication methods and practicing good computer security," the NSA said in an interview with AdAge.com. The posters will be distributed to military installations around the world and similar ads will appear in military publications, the NSA says.

Category 37 Education in security & ethics

2002-06-06 education students technical support reliability maintenance hands-on budgets

unding

NewsScan

#### STUDENTS PROVIDE BULK OF TECH SUPPORT IN SCHOOLS

Fifty-four percent of U.S. schools rely on students to provide technical support for their computer systems, according to a report titled "Are We There Yet?" (http://www.nsbf.org/thereyet/index.htm), released yesterday by the National School Boards Foundation. In 43% of the 811 districts surveyed, students troubleshoot for hardware, software and other problems, and 39% of the districts, students are tasked with setting up equipment and wiring. Nearly as many districts also report that students perform technical maintenance. The fact that students are providing so much hands-on assistance is viewed as a "win-win" situation by John Bailey, director of education technology for the Department of Education. Their tech savvy helps compensate for a dearth of tech support funding in school budgets and teachers who are "unevenly prepared for using technology as a tool for teaching and learning," according to the NSBF, which reports that 69% of the survey respondents rated new teachers as average or novices in computer skills. The role reversal signals a shift in the relationship between teachers and students as online lessons become integrated into the school curriculum, says Anne Bryant, executive director of the National School Boards Association: "Teachers become the guide on the side, instead of the sage on the stage." (AP 5 Jun 2002) http://apnews.excite.com/article/20020605/D7JV8EP00.html

Category 37 Education in security & ethics

2002-07-12 graduate studies information assurance INFOSEC

NewsScan

#### GRAD PROGRAM IN INFORMATION ASSURANCE OFFERED VIA NET

Norwich University is offering an 18-month master's degree program in Information Assurance (MSIA) intended to appeal primarily to candidates who are currently working in the information technology sector and who can consecrate an average of 12-15 hours a week to reading, online discussions, essays, and research about information technology. Because the program is carried out using asynchronous Web-based instruction, candidates from around the world are invited to apply. http://www3.norwich.edu/msia/

Category 37 Education in security & ethics

2002-08-01 criminal hackers crackers infrastructure protection infowar information warfare

homeland defense education ethics

NewsScan

### HACKERS ARE GOOD, CRACKERS ARE BAD

Richard Clarke, President Bush's cybersecurity czar, sees a big difference between online vandals (also called "crackers") who hack into systems for malicious purposes, and true hackers and security professionals who explore security holes that weren't found by the software maker. In fact, Clarke regards hacking as an obligation. He's told a group of hackers: "Some of us, here in this room, have an obligation to find the vulnerabilities." (AP/USA Today 31 Aug 2002)

Category 37 Education in security & ethics

2002-08-21 piracy intellectual property parents education awareness laws penalties

NewsScan

# JUSTICE OFFICIAL CALLS NET "THE WORLD'S LARGEST COPY MACHINE"

The U.S. Justice Department is gearing up to prosecute peer-to-peer pirates, warned Deputy Assistant Attorney General John Malcolm on Tuesday. Malcolm said Americans should realize that swapping illicit copies of songs and movies is a criminal offense punishable by prison terms. "A lot of people think these activities are legal, and they think they ought to be legal," Malcolm told attendees at the Progress and Freedom Foundation's annual meeting. "There does have to be some kind of a public message that stealing is stealing is stealing, whether it's done with sleight of hand by sticking something in a pocket or it's done with the click of a mouse." A few weeks ago, some members of Congress pressured the Justice Department to invoke the 1997 No Electronic Theft (NET) Act against P2P users who swap copyrighted files without permission. Under the Act, it is a federal crime to share copies of copyrighted products, such as software, movies or music, worth more than \$1,000 with anyone -- even friends or family members. Violations are punishable by one year in prison and by "not more than five years" in prison for works valued above \$2,500. "Most parents would be horrified if they walked into a child's room and found 100 stolen CDs? However, these same parents think nothing of having their children spend time online downloading hundreds of songs without paying a dime," said Malcolm. Meanwhile, Gary Shapiro, head of the Consumer Electronics Association, said there should be a distinction drawn between stealing real property and copying intellectual property. "When you copy intellectual property, there may or may not be harm. They assume that every copy made is a copy lost. That's not always the case." (AP 20 Aug 2002 & CNet News.com 20 Aug 2002)

http://apnews.excite.com/article/20020821/D7LHFC182.htm

http://news.com.com/2100-1023-954591.html

Category 37 Education in security & ethics

2002-09-26 intellectual property theft piracy education awareness campaign ethics

NewsScan

#### MUSIC ARTISTS SLAM DOWNLOADING

Record labels are using the talents of dozens of big-name recording stars, including Madonna, Sting and Britney Spears, in a multi-million-dollar ad campaign designed to shame people out of illegally swapping their songs. "Would you go into a CD store and steal a CD?" asks Spears. "It's the same thing -- people going into the computers and logging on and stealing our music." The new ad campaign is one facet of a multipronged approach aimed at quashing illegal file-swapping. The Recording Industry Association of America has also sued several file-swapping sites, threatened to crack down on companies and individual file-swappers, and lobbied for legislation that would mandate anti-copying technology in new products. Meanwhile, a KPMG study recently released said that instead of fighting Internet piracy, the recording industry would be better served by devoting more time to developing new Internet business models. (CNet News.com 25 Sep 2002) http://news.com.com/2100-1023-959537.html

Category 37 Education in security & ethics

2002-09-26 security education children government infrastructure protection schools kids

NewsScan

#### DEWIE THE TURTLE COMES OUT FOR COMPUTER SECURITY

In the tradition of Smokey the Bear's campaign for fire safety, the new cartoon figure Dewie the Turtle is being promoted by the Federal Trade Commission to teach kids and their parents of the importance of computer and network security (http://www.ftc.gov/infosecurity). Dewie urges the selection of hard-to-guess passwords, the use of antivirus software and computer firewalls, and other security practices. Do as Dewie says or you'll be sorry. (San Jose Mercury News 25 Sep 2002)

Category 37 Education in security & ethics

2002-10-11 intellectual property copyright piracy education ethics universities P2P peer-to-peer

privacy

NewsScan

# COLLEGES TOLD STUDENT PIRACY "OUT OF CONTROL"

A letter sent to more than 2,000 university presidents by the Recording Industry Association of America (RIAA) and the Motion Picture Association of America (MPAA) says: "We are concerned that an increasing and significant number of students are using university networks to engage in online piracy of copyrighted creative works. We believe there must be a substantial effort, both disciplined and continuous, to bring this piracy under control... Students must know that if they pirate copyrighted works they are subject to legal liability. It is no different from walking into the campus bookstore and in a clandestine manner walking out with a textbook without paying for it." (Cnet 11 Oct 2002) http://news.com.com/2100-1023-961637.html

#### COLLEGES URGED NOT TO MONITOR PEER-TO-PEER SHARING

The Electronic Privacy Information Center (EPIC), a Washington-based nonprofit organization that promotes freedom of speech on the Internet, is attacking letters recently written by the recording industry asking college officials to monitor Web use at their institutions for copyright violations made through peer-to-peer sharing of music or video files by members of the academic community. EPIC is criticizing those letters for trying to shift the burden of content enforcement to academic institutions which have scarce resources for such purposes, and is warning against a network "arms race" between file sharers and copyright enforcers. The group thinks colleges should avoid adopting a "confrontational role with respect to these technologies," because all it would do would be to harm the network's overall performance. (IDG News Service 11 Nov 2002) http://www.idg.com.hk/cw/readstory.asp?aid=20021111002

Category 37 Education in security & ethics

2002-11-27 university students policies copyright infringement intellectual property education

ethics violations

NewsScan

#### STUDENTS EVADE UNIVERSITY TACTICS TO PROTECT MEDIA FILES

As colleges and universities across the country take steps to rein in rampant unauthorized file downloading, students are ignoring policy changes that discourage such activities and are becoming more adept at circumventing technology blockades. "If you don't know how to do it, other people will just tell you," says one student. "There's not much they can do to stop you." And while university administrators are moving to placate entertainment companies complaining of student abuses, there's a pragmatic motivation at work as well — a large portion of most universities' bandwidth is being devoured by students' insatiable demand for online entertainment. Schools have closed off file-trading portals such as Kazaa, but the newest version of the Kazaa software includes a "port-hopping" feature that automatically seeks out open ports for its downloading activities. "It's an ongoing battle," says one network administrator. "It's an administrative nightmare trying to keep up." Meanwhile, schools appear conflicted in their quest for more ethical behavior among their students. "The biggest problems that universities are having is they have not openly decided whether their primary responsibility in this regard is law enforcement or education," says Virginia Rezmierski, who teaches in the University of Michigan's School of Information and recently surveyed universities on their monitoring practices. "Right now they're doing more monitoring than education." (New York Times 27 Nov 2002)

# 38.1 Consumer profiling

Category 38.1 Consumer profiling

2002-02-21 consumer privacy contract tracking surveillance vehicle automobile rental GPS

Geographical Positioning System

NewsScan

#### RENT-A-CAR COMPANY WILL CONTINUE SPYING ON SPEEDERS [9 Jul 2001]

Acme Rent-a-Car in New Haven has rebuffed the Connecticut Department of Consumer Protection and plans to continue using Global Positioning System (GPS) technology to track individuals who speed in rented vehicles, and levy fines on them of \$150 if the speeding continues for more than two minutes. The consumer agency's complaint against Acme is based not on privacy issues but on the charge that Acme's rental contract didn't give adequate information about what it was doing. (USA Today 9 Jul 2001)

http://www.usatoday.com/life/cyber/tech/2001-07-09-rental-car-tracking.htm

#### CAR RENTAL AGENCY CITED FOR SPYING ON SPEEDERS [21 Feb 2002]

Acme Rent-a-Car, based in Connecticut, has been cited by the state's Consumer Protection Commission for its practice of tracking customers' driving habits via GPS devices and assessing customers \$150 each time they exceeded 79 miles per hour. The commission said the company violated Connecticut's unfair trade practices act by not notifying customers of the monitoring, and ordered Acme to pay back "every single customer who they took money from illegally." Many car rental agencies use GPS to locate their vehicles in case they are stolen or taken out of the country. (Reuters/CNet 21 Feb 2002) http://news.com.com/2100-1040-842821.html

Category 38.1 Consumer profiling

2002-03-28 privacy survey Web sites e-commerce control

NewsScan

# WEB SITES COLLECTING LESS PERSONAL DATA

Many commercial Web sites are cutting back on the amount of personal data they regularly collect on visitors, with 84% of the 85 sites polled reporting that they're gathering less data than they did two years ago. That said, most of the sites -- 96% -- still collect at least some data from users, according to a survey conducted for the Progress and Freedom Foundation. The survey included such popular Web sites as Amazon, Google and Travelocity. Foundation President Jeffrey Eisenach said that the responses indicated a trend toward giving consumers more control over how their private information is used: 93% of the Web sites surveyed gave users the option of restricting the sale or transfer of their information to other businesses, up from 77% in 2000, and some 72% of sites promised consumer data would be secure, up from 48% the year before. (Wall Street Journal 28 Mar 2002)

http://online.wsj.com/article/0,,SB1017247161553469240.djm,00.html (sub req'd)

Category 38.1 Consumer profiling

2002-03-30 privacy preferences management policy junk mail spam advertising preferences

RISKS 22 02

In March 2002, Yahoo Groups caused a ruckus among its subscribers by unilaterally resetting all its members privacy preferences from NO to YES. Every member had to manually unsubscribe all over again.

Category 38.1 Consumer profiling

2002-08-27 consumer profiling cookies monitoring Web surfing legal agreement

NewsScan

### WEB AD COMPANY WILL NOW TELL YOU ABOUT YOUR SURFING PROFILE

Bringing an end to a 30-month investigation by 10 states charging improper use of profiles on network users, the Web advertising firm DoubleClick has agreed to provide consumers with better disclosure of what they're doing and to give them access to their own profiles. As part of the agreement, DoubleClick will pay a \$450,000 fine. Some privacy advocates say the agreement falls short of what is needed, because it still allows the company to create individual profiles, even though it must now openly acknowledge what it is doing. (Washington Post 27 Aug 2002)

Category 38.1 Consumer profiling

2002-09-30 consumer profiling privacy policy e-commerce

NewsScan

#### AMAZON CHANGES ITS TUNE ON PRIVACY POLICY

E-commerce giant Amazon has bowed to the wishes of a coalition of state attorneys general and is changing its privacy policy to make it more consumer-friendly. The changes mean the online retailer will provide consumers with information on what specific personal data is being collected, as well as examples of how it might be used. In addition, Amazon says it will not sell its customer database to marketers and will close some loopholes in its policy. Massachusetts Attorney General Thomas Reilly, who spearheaded the group of 16 states and the District of Columbia, said of the changes: "It's extremely important for all companies -- especially Internet sellers -- to handle consumer data carefully and confidentially." However, Junkbusters president Jason Catlett dismissed the changes as mostly cosmetic and called for an independent audit of Amazon's practices. Meanwhile, a report by Forrester Research estimates that consumers' concerns over privacy cost online retailers \$15 billion in lost sales in 2001. "It's still right up there on the front of consumers' minds, so anything Amazon and others can do to soothe those fears is important," says Forrester analyst Christopher Kelley. (E-Commerce Times 27 Sep 2002) http://www.ecommercetimes.com/perl/story/19525.html

# 38.2 Trade in personal information

Category 38.2 Trade in personal information

2002-05-02 privacy surveillance wireless communication phone location position service

NewsScan

#### SWEDISH CELL PHONE USERS CAN PINPOINT FRIENDS' LOCATIONS

Customers of Sweden's Telia Mobile have a new way to find out where their friends are -- by using their cell phone. The service, called friendPosition, uses graphic and text messages to reveal the locations of other users. Both people -- the seeker and the sought -- must be using specially enabled cell phones equipped with wireless location services. The friendPosition service could prove a boon to Telia, which, like other wireless carriers, is looking for ways to boost average revenues per user. The \$2 a month charge may not seem like much, but could be critical in an industry with very slim profit margins. Meanwhile, similar services could be heading this way, says one analyst: "Commercial location services will be available here by the end of the year," predicts Al Fross, a principal at Pelorus Group. He estimates that global revenue from wireless location services could reach \$3.2 billion by 2006. (Investor's Business Daily 2 May 2002)

Category 38.2 Trade in personal information

2002-09-05 privacy public records Web Internet freedom information access

NewsScan

# DO ME A FAVOR, OPEN THE DOOR, AND LET 'EM IN, OOH YEAH

So just who is that knocking that door and ringing that bell? In Hamilton County, Ohio, trouble has flowed from the decision of the clerk of courts to make all public records freely available on the Web. (They were already available to anyone who would go to the county courthouse.) The official explained: "It was the natural progression of technology. Everything we get is scanned and available. It was very easy to open the door to the public." And so now anyone can look on the Web to see anyone else's state tax liens, arrest warrants, bond posting, etc. People are searching the records to find out the dirt on their neighbors - or just to get copies of the floor plans of their houses. Bank executive Jim Moehring says, "You do kind of feel like Big Brother because you can look right in and get into what everyone's doing." The clerk of courts says ruefully: "We didn't realize we were walking into a hornet's next until after we were under way. " (New York Times 5 Sep 2002)

# 38.3 Industry efforts for privacy protection

Category 38.3 Industry efforts for privacy protection

2002-02-05 e-commerce trust certification reliability credibility fraud online shopping

NewsScan

### BETTER BUSINESS BUREAU TARGETS ONLINE PRIVACY WITH NEW SITE

The Better Business Bureau has launched a new Safe Shopping Web site that enables consumers to locate online companies that have met BBB standards for privacy in e-commerce. Visitors to

http://www.bbbonline.org/consumer/ will find nearly 11,000 Web sites that have earned one or both of the BBBOnline Privacy and Reliability seals. A recent survey showed that almost 90% of consumers would feel safer making a purchase from an online company that displays one of the seals than from a company that does not, according to Greenfield Online. "The BBB system will encourage the business community to step up to the plate and meet consumer expectations regarding online privacy," says Ken Hunter, president and CEO of the Council of Better Business Bureaus and BBBOnline. (E-Commerce Times 4 Feb 2002)

http://www.ecommercetimes.com/perl/story/16149.html

Category 38.3 Industry efforts for privacy protection

2002-04-04 privacy policy interpretation tool translation alert freeware

NewsScan

#### IBM AND AT&T GIVE AWAY WEB PRIVACY SOFTWARE

IBM is now giving away its Tivoli Privacy Wizard software, which transforms a Web [site's] written privacy policies into electronic guidelines for its own employees, and AT&T is giving away software that will alert Web surfers to different privacy settings on sites they visit. Internet users have consistently have consistently rated privacy issues high on their list of concerns about the Web. IBM acknowledges the skepticism of some privacy advocates and admits that the donated software won't deter deliberate privacy violations, but insists that it "may help reduce the all-too-frequent accidents in privacy" caused by a company's employees failing to understand or follow the company's written privacy policies. (Reuters/San Jose Mercury News 4 Apr 2002)

http://www.siliconvalley.com/mld/siliconvalley/2997058.htm

# 38.5 EU legislation & regulation concerning privacy

Category 38.5 EU legislation & regulation concerning privacy

2002-05-28 privacy international concerns .NET e-commerce access

NewsScan

#### EUROPEAN COMMISSION HAS PRIVACY CONCERNS ABOUT MICROSOFT

The European Commission says Microsoft's .NET Passport system may be in violation of the Commission's data protection law. Passport stores a user's ID information on company servers so it doesn't have to be reentered as the user moves from site to site on the Web. The EU is fearful both that personal data might be passed to unknown parties and also that failure to register with Passport could exclude people from visiting some sites. (New York Times 28 May 2002) http://partners.nytimes.com/2002/05/28/technology/28SOFT.html

Category 38.5 EU legislation & regulation concerning privacy

2002-05-28 consumer data privacy Europe directive e-payment penalties fines

FindLaw Download This 87

In May 2002, the European Union warned that Microsoft faced possible fines for violating the EC Data Protection Directive. Microsoft's .NET Passport service may have failed to protect consumer privacy at the standards required in Europe.

Category 38.5 EU legislation & regulation concerning privacy

2002-06-04 homeland security international Europe privacy data protection terrorism surveillance privacy

1 V

FindLaw Download This 88

#### EU PANEL OKS PRIVACY RULES

The European Union Parliament passed weakened data protection and privacy rules Thursday, bowing to pressure from EU governments eager to boost controls in its fight against terrorism. The new legislation, which still faces final approval by the 15 EU governments, will give anti-terrorist investigators greater powers to eavesdrop on private data on the Internet and other electronic records like people's phone calls.

http://news.findlaw.com/ap\_stories/high\_tech/1700/5-30-2002/20020530060005\_11.html

Cyberspace Privacy Resources

http://www.findlaw.com/01topics/10cyberspace/privacy/

Category 38.5 EU legislation & regulation concerning privacy

2002-06-06 privacy international Europe e-mail cookies surveillance permission opt-in

Security Wire Digest 4 44

# \*E.U. PARLIAMENT RESTRICTS COMMERCIAL USE OF PERSONAL DATA

Companies will need permission to send unsolicited commercial e-mail or use cookies in Internet browser software under a series of amendments to the European Union's data privacy law. E.U. Parliament members last week ignored a committee's recommendations against the restrictions, choosing instead to require companies to get permission from users before they can send unsolicited e-mail, or spam. The Citizens' Rights Committee wanted member states to dictate opt-in policies for including users on third-party mailing lists. The amendment is expected to become law by the end of the year. Member states still can adopt their own laws on how to use personal information, rather than be forced to delete customer data within a specific time frame.

Category 38.5 EU legislation & regulation concerning privacy

2002-08-20 surveillance spying privacy Europe regulations legislation e-mail phone

NewsScan

#### GROUP WARNS OF EU SURVEILLANCE

Statewatch, a U.K. group dedicated to protecting civil liberties on the Internet, is warning that European governments are planning changes to the 1997 EU Directive on privacy in telecommunications that would require phone companies, mobile network operators and ISPs to store details of their customers' Web use, e-mails and phone calls for between one to two years. Current law states that traffic data may be retained for billing purposes only and then must be deleted. "EU governments claimed that changes to 1997 EC Directive on privacy in telecommunications to allow for data retention and access by the law enforcement agencies would not be binding on member states -- each national parliament would have to decide. Now we know that all along they were intending to make it binding, compulsory across Europe," says Tony Bunyan, editor of Statewatch. The changes may include the provision that police would need a judicial order before accessing traffic data, but Statewatch warns that such conditions have been sidestepped before. (CNet News.com 20 Aug 2002) http://news.com.com/2100-1023-954487.html

Category 38.5 EU legislation & regulation concerning privacy

2002-08-30 consumer individual privacy Europe USA Web data subject directive online ecommerce

NewsScan

# TOUGH EU PRIVACY RULES INFLUENCE U.S. WEB PRACTICES

Europe's strict approach to consumer data protection is forcing many U.S.-based companies to follow suit in order to continue serving their European customers. "Europeans are extremely concerned about the use of data about people," says Rockwell Schnabel, the U.S. ambassador to the European Union. "The data privacy issue is a huge issue over there. American partners have to live with those rules, and they can't do with it what they can with American data." A case in point is Microsoft's Passport online ID service that enables users to log in once and then move from one secure Web site to another. Consumer and privacy groups had accused Microsoft of not taking adequate steps to protect consumers' personal information and in a settlement earlier this month, Microsoft admitted no wrongdoing, but agreed to government oversight of its consumer privacy policies for the next 20 years. A separate Passport investigation by the EU is still pending. "The EU directive raised the bar on the practices by U.S. companies for U.S. consumers," says Marc Rotenberg, head of the Electronic Privacy Information Center. "Passport is a good example of that, because Microsoft is very much aware that its products are going to have to meet EU privacy standards." EU standards specify that data may be collected only for "specified, explicit and legitimate purposes, and to be held only if it is relevant, accurate and up to date." Citizens may access any data about themselves, find out its source, correct inaccuracies, and pursue legal recourse for misuse. (San Jose Mercury News 29 Aug 2002)

# 38.6 US legislation & regulation concerning privacy

Category 38.6 US legislation & regulation concerning privacy

2002-02-19 sex offender public list privacy anonymity constitutionality judicial review lawsuit

NewsScan

#### ONLINE SEX-OFFENDER LISTS TO BE GIVEN CONSTITUTIONAL SCRUTINY [19 Feb 2002]

The U.S. Supreme Court will decide the question of whether the Constitution allows states to pass legislation enabling the use of Internet registries of convicted sex offenders who have served their time in jail and been released back into society. All states have some version of a sex-offender law, which typically allows publication of a convicted offender's name, address, and other personal information. Such laws are deemed to conform to the Constitution if they are narrowly focused on public safety and not used to extend the punishment of someone beyond what was prescribed by the sentence given to him by the courts, because it is unconstitutional to punish someone twice for the same crime. (AP/USA Today 19 Feb 2002) http://www.usatoday.com/life/cyber/tech/2002/02/19/scotus-sex-offender-registries.htm

Category 38.6 US legislation & regulation concerning privacy

2002-04-19 privacy legislation proposal bill personal information EU directive opt-in

NewsScan; http://news.com.com/2100-1023-886679.html

#### INTERNET PRIVACY

Sen. Ernest Hollings (D-S.C.) has introduced an online privacy bill that would require companies to obtain explicit permission from people before collecting and sharing their personal information. The Online Personal Privacy Act reflects some components of the recently ratified European Union privacy directive, requiring that individuals "opt-in" to any collection, use or disclosure of "sensitive information." Sensitive information is defined as relating to any financial, medical, ethnic or religious affiliation, sexual orientation or political data. In addition, the bill would require businesses to provide an "opt-out" option when collecting nonsensitive information, such as that related to online clothing purchases. "Privacy fears are stifling the development and expansion of the Internet as an engine of economic growth," says Hollings. (CNet News.com 18 Apr 2002)

Category 38.6 US legislation & regulation concerning privacy

2002-05-03 identify theft proposed legislation bill penalties

NewsScan; http://www.washingtonpost.com/wp-dyn/articles/A24368-2002May2.html

### ASHCROFT WANTS STIFFER PENALTIES FOR IDENTITY THEFT

U.S. Attorney General John D. Ashcroft is proposing legislation increasing by 2 to 5 years the jail time for persons convicted of aggravated identity theft a crime. "The Department of Justice is committed to seeing to it that criminals and terrorists cannot find refuge in the identities of law-abiding citizens of this country." Since October 1998, 2,223 criminal cases have been filed against 2,899 defendants. The call for tougher penalties won immediate support from Democrat Sen. Dianne Feinstein of California, who chairs the Senate Judiciary subcommittee on technology, terrorism and government. (Washington Post 3 May 2002)

Category 38.6 US legislation & regulation concerning privacy

2002-05-17 data collection Web privacy commercial information proposed law legislation bill

NewsScan

#### ONLINE PRIVACY BILL DELAYED

Parliamentary maneuvering has delayed consideration of a Senate bill that would protect individual privacy on the Internet and regulate how businesses may use customer e-mail addresses and other personal data. The proposed legislation would also limit how businesses may use phone numbers, purchase records, and other data collected through their Web sites, and would require online businesses to get customer permission before collecting or sharing sensitive personal information. "What we are proposing simply codifies businesses' best practices on the Internet," Hollings says Senator Ernest Hollings (D-SC), who sponsored the bill. (Reuters/USA Today 16 May 2002)

http://www.usatoday.com/life/cyber/tech/2002/05/16/privacy-bill.htm

Category 38.6 US legislation & regulation concerning privacy

2002-05-21 Internet privacy proposed law legislation bill

FindLaw Download This 86

#### VENTURA MULLS INTERNET PRIVACY BILL

Minnesota's Senate and House overwhelmingly approved a bill that backers say would make the state the first to give Internet users control over whether service providers disclose their personal information. Gov. Jesse Ventura will now decide its fate. He has not indicated a position on the bill. . . Under the bill, ISPs would have to tell Minnesota consumers whenever they plan to disclose such personal information about them as which Web sites they've visited, their e-mail or home addresses or telephone numbers. They also would have to say how the information would be used.

http://news.findlaw.com/ap/ht/1700/5-20-2002/20020520050002\_6.html

"The Body" Ponders His Next Move

http://www.canoe.ca/SlamWrestlingVentura/venturap1.html

Category 38.6 US legislation & regulation concerning privacy

2002-05-28 Internet privacy surveillance

FindLaw Download This 87

#### GOVERNOR SIGNS INTERNET PRIVACY BILL

Internet users will be able to control whether their service providers disclose their personal information under a new Minnesota law that could speed federal action on Internet privacy. National Internet companies fought the bill, signed by Gov. Jesse Ventura on Wednesday, and its authors described it as the most comprehensive state Internet privacy law. It won't take effect until March. The law requires ISPs to tell Minnesota consumers whenever they plan to disclose such personal information as which Web sites users have visited, their e-mail or home addresses or their telephone numbers. They also would have to say what the information would be used for.

http://news.findlaw.com/ap/ht/1700/5-22-2002/20020522210004\_13.html

FindLaw's Minnesota Legal Resources

http://www.findlaw.com/11stategov/mn/index.html

Category 38.6 US legislation & regulation concerning privacy

2002-06-03 financial institutions banks confidential information monitoring money-laundering alert suspicious activity privacy surveillance

NewsScan; http://www.washingtonpost.com/wp-dyn/articles/A49323-2002Jun2.html

### PATRIOT ACT TESTS PRIVACY BOUNDARIES

The post-September 11th antiterrorism legislation known as the USA Patriot [Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism] Act, which enlists financial institutions in an effort to identify money-laundering and terrorist funding, has caused concern among some civil libertarians because the legislation gives law enforcement and intelligence agencies greater access to confidential information without a subpoena. And last week the Treasury Department's Financial Crimes Enforcement Network (FinCen) began operating a secure online network to make it easier for financial firms to alert the government to suspicious customer activity. FinCen director James F. Sloan says that suspicious-activity reports, complemented by the agency's data warehouses and mining tools, have identified terrorist suspects, and have led to "an opportunity to work with the industry like never before." (Washington Post 3 Jun 2002)

Category 38.6 US legislation & regulation concerning privacy

2002-06-12 privacy opt-in financial information confidentiality political activism

PoliTech, http://www.aclu.org/news/2002/n061202a.html

An ACLU press release began as follows in June 2002:

NEW YORK--The American Civil Liberties Union today congratulated the people of North Dakota for defending their privacy by rejecting a ballot measure that would have allowed banks to share customers' information without their permission. "This vote was a stunning defeat for the powerful financial companies who were trying to bamboozle the citizens of North Dakota into acting against their own interests," said Jennifer Ring, Executive Director of the ACLU of the Dakotas. ...

"The results in North Dakota are significant not just in that state but nationally," said Barry Steinhardt, Director of the ACLU's Technology and Liberty Program. "If the voters in a small midwestern state vote for privacy by more than a three-to-one margin despite an intense media campaign urging them not to, then politicians in Washington and Sacramento and Albany ought to be listening."

"The pro-privacy campaign was waged by a group of citizen-volunteers led by Charlene Nelson, a homemaker and mother of three working out of her home in Casselton. Until a last-minute \$25,000 contribution by the ACLU for radio ads, the privacy forces had reported donations of just \$2,450."

# 38.7 Other legislation & regulation concerning privacy

Category 38.7 Other legislation & regulation concerning privacy

2002-03-12 privacy warnings disclaimers UK law legislation legal requirements monitoring

surveillance workplace e-mail communications

RISKS 21 95ff

Michael Bacon noted in RISKS the logical difficulties of warnings such as the BBC's e-mail disclaimer, "Please note that the BBC monitors e-mails sent or received. Further communication will signify your consent to this." If you reply to indicate that you don't consent, have you consented nonetheless? Is there any way to avoid consent and monitoring?

Further discussion in RISKS explained that the disclaimer was required for compliance with UK privacy laws. J. F. Hitches explained, >That sort of statement will be seen more widely on messages coming from the UK because it is part of a requirement of an Act of Parliament called the "Regulation of Investigatory Powers Act". This is combined with a Statutory instrument called "The Telecommunications (Lawful Business Practice Regulations) 2000".

The requirement is that monitoring may only be carried out "if the controller of the telecommunications system on which they are effected has made all reasonable efforts to inform potential users that interceptions may be made".<

Category 38.7 Other legislation & regulation concerning privacy

2002-04-08 privacy e-mail monitoring surveillance policies UK regulations international

NewsScan

#### ROUTINE E-MAIL MONITORING BANNED IN UK OFFICES

A new code defining workers' privacy rights prohibits British employers from routinely monitoring e-mail and Internet usage in UK offices, even when there is "reason to believe" that they are personal and sent or received on a work computer during business hours. The code reflects the standards on monitoring that the Information Commission, the UK's data protection watchdog, says must be met in order to comply with the country's Data Protection Act. The commission has threatened to take action against companies that violate the new code. Industry groups have protested the code, with one human resources manager saying that "It's overly concerned with the employee's privacy it is still far too prescriptive and just not realistic." (Financial Times 7 Apr 2002)

http://news.ft.com/news/industries/internet&e-commerce

Category 38.7 Other legislation & regulation concerning privacy

2002-06-18 International UK Britain privacy e-mail cellular mobile telephone surveillance law law enforcement government agencies Internet eavesdropping

FindLaw Download This 90

# BRITAIN RETHINKS NET SURVEILLANCE

The British government said Tuesday it was withdrawing a heavily criticized plan to give more bureaucrats and local authorities the power to monitor private e-mail and mobile telephone records. Civil liberties groups and opposition politicians had condemned the proposed changes to the Regulation of Investigatory Powers Act, which they dubbed a "snoopers' charter." Under the act, passed by Parliament two years ago, the police, intelligence agencies, Customs and Excise and the Inland Revenue Service have the authority to demand records of e-mail, mobile phone and Internet traffic. http://news.findlaw.com/ap/ht/1700/6-18-2002/20020618084502\_01.html

# UK Legal Resources

http://www.findlaw.com/12international/countries/uk/index.html

Category 38.7 Other legislation & regulation concerning privacy

2002-08-06 universal identifier citizen international privacy identity

NewsScan

# JAPANESE SAY THEY DON'T WANT TO BECOME NUMBERS

Japan's creation of a new citizen database has caused widespread concern that there has not been enough attention paid to privacy issues. Every citizen, starting at birth, will be assigned a unique 11-digit number. At present it will be used only to retrieve basic information (name, address, sex, and birth date), but many people think the system will be expanded to include other personal data. The new system has prompted widespread disobedience in the country, and half a dozen cities have refused to have any part of it. Nobuo Hoshino, mayor of Yokubunji, presiding over a "disconnecting ceremony," said: "Residents are sending us their views by e-mail, fax and various other ways, and almost all of them support us." One critic says that the project will grow and grow into "a bigger project, named 'E-Government,' that will have 16,000 administrative uses." (New York Times 5 Aug 2002)

# 38.8 Law enforcement & privacy

Category 38.8 Law enforcement & privacy

2002-02-13 surveillance cameras law enforcement police crime prevention anonymity public

expectation privacy

# NewsScan

#### WASHINGTON POLICE EXPAND USE OF SURVEILLANCE TECHNOLOGY [13 Feb 2002]

Noting that people in the United Kingdom have "easily adapted" to pervasive public surveillance and that "there has not been an outcry about privacy there," Washington, D.C. police officials are busy expanding the public use of surveillance cameras. A police department spokesman says, "In the context of September 11, we have no choice but to accept the greater use of this technology." MIT emeritus sociology professor Gary T. Marx concedes that "almost all of the surveillance innovations are easily justifiable" but worries that "the major concern is: where is it leading?" (Wall Street Journal 13 Feb 2002) http://online.wsj.com/ (sub req'd)

Category 38.8 Law enforcement & privacy

2002-11-20 infrastructure protection homeland security legislation law bill privacy surveillance

wiretaps court order probable cause

#### NewsScan

#### HOMELAND SECURITY GIVES GOV'T NEW POWERS

Provisions of the legislation to create the U.S. Department of Homeland Security bill would allow Internet service providers to give the government more information about their subscribers and give police new Internet wiretap powers. The Electronic Privacy Information Center and other civil liberties groups say the bill's language lets Internet providers reveal subscriber information to any government officials, not just investigators. Another section of the bill gives U.S. authorities new power to trace e-mails and other Internet traffic during cyber attacks without first obtaining even court approval in the event hat there occurs "an immediate threat to national security" or an attack against a "protected computer." (AP/New York Times 20 Nov 2002)

# 38.9 Surveillance

Category 38.9 Surveillance

2002-03-05 anonymizer quality assurance QA compromise vulnerability design flaw analysis

RISKS, http://www.cs.bu.edu/techreports/pdf/2002-003-deanonymizing- 21 93 safeweb.pdf

David Martin of Boston University reported on his group's analysis of the SafeWeb anonymizer service (which went out of business in December 2001 but whose technology was licensed to other firms). The analysis showed that the service did protect anonymity. However, despite the company's assurances about security, in fact the service opened users to serious compromise through errors in the service's design.

The simplicity of the errors is startling. Martin summarizes the situation as follows (quoting):

>First a quick SafeWeb overview: a SafeWeb user types in a URL. It goes to safeweb.com within an SSL connection; SafeWeb sanitizes the requested content and delivers it back to the browser. The origin server Web site only sees a connection from safeweb.com, and eavesdroppers near the user only see an encrypted connection to safeweb.com On-screen, SafeWeb uses frames to separate the SafeWeb controls from the requested content. Let's call them the "control" and "content" frames.

#### Now let's meet the protections:

- (1) simultaneously open windows or frames can only communicate with each other if they're from the same domain,
- (2) scripts stop running when a new page is displayed, and
- (3) cookies are available only to the domain that set them.

The problem is that both of SafeWeb's frames are served from the same tunnel (https://www.safeweb.com/) even though their content comes from radically different sources: the trusted SafeWeb site on the one hand, and the untrusted third party site on the other. Since both frames come from the same domain, the Web browser exposes each Document Object Model to the other: protection #1 is gone.

Since the control frame is basically static, it's a great place for an attacker to tuck away any code that needs to persist throughout the browsing session -- like spyware. So protection #2 is gone too.

SafeWeb also wanted to support pseudonymous persistent cookies. Since the content frame is always associated with a single privacy domain, they aggregated all of the pseudonymous cookies from sites a user might visit through SafeWeb into one "master cookie" associated with the fixed domain safeweb.com. That way, the individual cookies all get stored on the user's computer in a slightly different form, and SafeWeb doesn't have to maintain any persistent state on their servers (and users don't have to log in to SafeWeb, etc.). But this approach discards protection #3 as well.

To exploit these lost protections, an attacker has to take control of one of the frames: the content frame is the obvious choice. That turns out to be not too hard. SafeWeb \*requires\* that JavaScript be enabled in the browser. Recognizing the risk, SafeWeb tried to sanitize scripts delivered to the content frame, but they didn't go nearly far enough. The result? By choosing to use this privacy enhancing system, users become vulnerable to having their IP address revealed, \*all\* of their cookies stolen, and the remainder of their privacy-"enhanced" browsing session silently transmitted to an attacker in spite of the layer of SSL protection. This is not speculation; we have tested several effective exploits against the system.<

[MK comments: You would think that the designers would have asked for outside analysis before implementing these designs, no?

MORAL #1: Challenge your own security models.

MORAL #2: Don't assume that vendors have challenged their own security models.]

Category 38.9 Surveillance

2002-04-22 surveillance privacy Web cameras Webcam hijack wireless

RISKS 22 04ff

Dave Farber noted in RISKS:

Thousands of people who have installed a popular wireless video camera, intending to increase the security of their homes and offices, have instead unknowingly opened a window on their activities to anyone equipped with a cheap receiver. The wireless video camera, which is heavily advertised on the Internet, is intended to send its video signal to a nearby base station, allowing it to be viewed on a computer or a television. But its signal can be intercepted from more than a quarter-mile away by off-the-shelf electronic equipment costing less than \$250. [...] [Source: John Schwartz, \*The New York Times\*, 14 Apr 2002 http://www.nytimes.com/2002/04/14/technology/14SPY.html?ex=1019744700&ei=1&en=cfeb1e93a276b9ee]

#### Marc Roessler commented:

"This is nothing new. Such cameras are even installed in some public restaurants and shops. Note that this basically voids all claims of the shop owners concerning privacy and data protection -- ANYONE can receive that data. And, as more and more cameras are installed, the risk of malicious "camera takeovers" rises significantly. Think about webcams, cams integrated into notebooks/cellular phones, car dashboards (detect the driver falling asleep). Those are easily tapped (or subverted, such as by installing trojan software/ firmware). this has some enormous potential. The case of the Nanny-Cams shows the deviousness of this kind of attack: as the devices are not suspected to be used to spy on their owner ("I own that device; that makes it trusted"), they function more or less as hidden cameras. For more "camera takeover" scenarios take a look at my paper "How to find hidden cameras" [1].

[1] http://www.franken.de/users/tentacle/papers/hiddencams.pdf

Category 38.9 Surveillance

2002-06-06 expectation privacy covert surveillance law moral obligations rights duties secrecy

RISKS 22 11

In France, a worried father installed a hidden camera in his own home to check on the behavior of his babysitter's boyfriend. The camera found no abuse, but it did record the baby sitter and her boyfriend having sex while the three-year-old slept in the next room. The father was arrested and fined for violating the couple's privacy. In a thoughtful analysis published in the Los Angeles Times, author Gary T. Marx commented that although such an outcome was unlikely in the USA because of less stringent privacy laws, "The fact that there is still a legal right to secretly record images in the U.S. does not mean that it is the right thing to do. We would do well to learn from the French the general principle of respect for private life, a principle that holds no matter what new technologies are offered to us that allow us to spy on others."

Category 38.9 Surveillance

2002-06-17 university campus e-mail government employees freedom-of-information laws

FOIA public records

# Edupage

# CAMPUS E-MAIL EXPOSED TO PUBLIC SCRUTINY

Many states identify administrators and professors at public colleges as state employees, potentially exposing their letters, documents, and e-mail to public scrutiny under freedom-of-information laws. Some institutions have begun to update policies to safeguard personal e-mail or warn professors to be careful what they write. Open-records laws don't specify clearly whether professors' research notes, lecture notes, or regular mail would qualify as public records, but most states assume that state employees' e-mail messages are public records, even when the law is ambiguous. Employees at private colleges can be exposed as well, although not through open-records laws; a person would need to obtain a court order or a subpoena, requiring involvement in litigation against the college. Chronicle of Higher Education, 17 June 2002 (sub. req'd) http://chronicle.com/free/v48/i41/41a03101.htm

Category 38.9 Surveillance

2002-09-05 surveillance law enforcement police database suspects associates

NewsScan

#### GUILT-BY-ASSOCIATION?

Law enforcement officials in Wilmington, Delaware are being criticized by privacy advocates for putting digital photos and other information into a database of associates of suspected drug dealers rounded up in rough neighborhoods. A Wilmington public defender calls it "guilt by association" and Barry Steinhardt of the ACLU charges: "They are stopping, searching and putting into a database photographs of people whose only crime is being in the wrong place at the wrong time. It's bad law enforcement, and it's bad for civil liberties." Police Chief Michael Szczerba's response is: "If you come into our city to take in a ballgame or dine at a restaurant or go to a theater, you likely won't know about these corner patrols. But if you come to sell drugs or drink alcohol on the corner or just be a general nuisance, you're going to see us." (USA Today 4 Sep 2002) http://www.usatoday.com/tech/news/2002-09-04-wilmington

Category 38.9 Surveillance

2002-09-05 surveillance civil liberties homeland security Internet monitoring freedom Europe USA international

#### NewsScan

#### BEWARE THE 'PREDATORS OF DIGITAL FREEDOMS'?

Reporters Without Borders, an international media-rights group, has accused several Western democracies of becoming "predators of digital freedoms" in their efforts to increase surveillance on the Internet as part of their fight against terrorism. "A year after the tragic events in New York and Washington, the Internet can be included on the list of 'collateral damage," said the group in a report. "Cyber-liberty has been undermined and fundamental digital freedoms have been amputated." The report cites recent moves to weaken individual privacy laws in the U.S., Britain, France, Germany, Spain, Italy and Denmark, as well as the European Parliament, that risk turning ISPs and telecommunications operators in those countries "into potential branches of the police." The report's findings mirror those in another report earlier this week issued by the Electronic Privacy Information Forum and Privacy International, which note that governments worldwide have made it easier for authorities to eavesdrop on telephone and online conversations in order to fight terror. (AP 5 Sep 2002) http://apnews.excite.com/article/20020905/D7LRJR200.htm

Category 38.9 Surveillance

2002-10-15 government wireless cellular phone mobile surveillance tracking identification monitoring

#### NewsScan

#### UK GOVERNMENT PLANS CELL PHONE TOWER TRACKING SYSTEM

The government of the U.K. is funding secret radar technology research that uses mobile phone masts to enable security officials to watch vehicles and people in real time almost anywhere in Britain. The Celldar technology, which works wherever there is cell phone coverage, "sees" the shapes made when radio waves emitted by the towers meet an obstruction. Signals bounced back by immobile objects, such as buildings and trees, are filtered out by the receiver, and what's left on the screen are images of anything that moves. When combined with technology that allows individuals to be identified by their mobile phone handsets, the Celldar system would enable security officials to locate and track a specific person from hundreds of miles away. An individual using one type of receiver, a portable unit a little bigger than a laptop, could even create a "personal radar space" around his or her location for security purposes. Researchers are also working on an "X-ray vision" feature that would enable the devices to "see" through walls and look into people's homes. UK Ministry of Defence officials are hoping to introduce the system as soon as resources allow, but civil liberties advocates have been quick to complain: "It's an appalling idea. The government is just capitalizing on current public fears over security to introduce new systems that are neither desirable nor necessary," says Simon Davies, director of Privacy International. (The Observer 13 Oct 2002) http://www.observer.co.uk/uk\_news/story/0,6903,811027,0

Category 38.9 Surveillance

2002-12-17 forensic investigation employee background

NewsScan

#### COMPUTER FORENSICS TARGETS DISGRUNTLED EMPLOYEES

"There's a growing acknowledgment among executives that insiders can do more damage than the smartest outside hacker," says a Manhattan systems administrator. With that in mind, computer forensics software is targeting employee habits and behavior in an effort to stop corporate crime before it happens. Products like Savvydata's RedAlert collect, consolidate and analyze employee information to determine an individual's threat to the organization, based on what files employees accessed, the contents of their e-mails, and which company policies they violated. That information can then be combined with RedAlert's subscription-based Intelligent Information Dossier service, which allows corporate IT folks to research workers' criminal histories, credit information, financial asset details, friends and associates. Some IT workers think RedAlert goes too far: "RedAlert totally freaked me out," says a systems administrator for a Wall Street firm. "I understand why you'd need something like this if you are the CIA, but for standard biz use? I just don't think I'd work at a company that used these sorts of tools." Meanwhile, other products such as EnCase Enterprise Edition scour the network to see if any workers possess "unauthorized information" in order to prevent problems such as fraud, future lawsuits and other issues. (Wired.com 13 Dec 2002)

# 41 Cryptanalysis techniques

Category 41 Cryptanalysis techniques

2002-05-14 smart card inference cracking confidentiality cryptography key vulnerability

NewsScan; http://www.newscientist.com/news/news.jsp?id=ns99992273

#### SMART CARDS REVEAL ALL DURING CAMERA FLASH

A flash of light can cause sensitive information stored on a smart card microprocessor to be revealed, say UK researchers at Cambridge University, who've found that firing light from an ordinary camera flash at parts of a smart card chip can assist a thief in determining the sensitive information stored on the card, including the cryptographic key used to secure financial transactions. The attack is described as "semi-invasive," as only part of a chip's protective covering must be removed in order to "flash" it. Meanwhile, another group at Cambridge has developed a microchip design that would resist this technique, using a more complex "asynchronous" microprocessor that would not respond in the same way to light interference. (New Scientist 13 May 2002)

## 42.1 Crypto algorithm weaknesses

Category 42.1 Crypto algorithm weaknesses

2002-02-15 wireless networks Wi-Fi 802.1x WEP vulnerabilities implementation man-in-themiddle attacks interception session hijacking

RISKS 21 92

From an article by Ephraim Schwartz in InfoWorld, Thursday, February 14, 2002 as reported in RISKS by Monty Solomon:

Researchers Claim to Crack Wi-Fi Security; Proponents deny wireless networking spec is vulnerable to hijack, authentication attacks.

A University of Maryland professor and his graduate student have apparently uncovered serious weaknesses in the next-generation Wireless Fidelity security protocol known as 802.1x. In a paper, "An Initial Security Analysis of the IEEE 802.1X Standard" funded by the National Institute of Standards, Professor William Arbaugh and his graduate assistant Arunesh Mishra outline two separate scenarios that nullify the benefits of the new standard and leave Wi-Fi networks wide open to attacks. The use of public access "hot spots" are particularly vulnerable to session hijacking because these locations do not even deploy the rudimentary Wired Equivalent Privacy protocol. "This problem exists whether you use WEP or not, but it is trivial to exploit if not using WEP," said Arbaugh.

#### Flaws Described

Dubbed "session hijacking" and "man-in-the-middle," both attacks basically exploit inherent problems in Wi-Fi as well as exploiting how the new 802.1x standard is designed. "Here's how session hijacking works. The hacker waits for someone to finish successfully the authentication process. Then you as the attacker send a disassociate message, forging it to make it look like it came from the AP [access point]. The client [user] thinks they have been kicked off, but the AP thinks the client is still out there. As long as WEP is not involved you can start using that connection up until the next time out, usually about 60 minutes," said Arbaugh. [...]

http://www.pcworld.com/news/article/0,aid,84424,00.asp

Category 42.1 Crypto algorithm weaknesses

2002-03-10 weak encryption vulnerabilities ICAT CVE

#### **ICAT** Metabase

The ICAT Metabase < http://icat.nist.gov/icat.cfm > for the Common Vulnerabilities and Exposures (CVE) database reported 10 vulnerabilities involving weak encryption out of a total of 1241 for the period from 1 Jan 2001 to 10 Mar 2002. This represents about 1% of all vulnerabilities logged for that period. Overall, for the entire period since the CVE began recording vulnerabilities in 1995, weak encrytion is named in 51 of the 3677 vulnerabilities or about 1% of the total. The vulnerabilities listed for 2001 and up to 10 Mar 2002 are as follows:

CAN-2001-1005: Starfish Truesync Desktop 2.0b as used on the REX 5000 PDA uses weak encryption to store the user password in a registry key, which allows attackers who have access to the registry key to decrypt the password and gain privileges. Published Before: 8/31/2001 Severity: Medium

CAN-2001-1003: Respondus 1.1.2 for WebCT uses weak encryption to remember usernames and passwords, which allows local users who can read the WEBCT.SVR file to decrypt the passwords and gain additional privileges. Published Before: 8/31/2001 Severity: Medium

CAN-2001-0983: UltraEdit uses weak encryption to record FTP passwords in the uedit32.ini file, which allows local users who can read the file to decrypt the passwords and gain privileges. Published Before: 8/31/2001 Severity: High

CAN-2001-0618: Orinoco RG-1000 wireless Residential Gateway uses the last 5 digits of the 'Network Name' or SSID as the default Wired Equivalent Privacy (WEP) encryption key. Since the SSID occurs in the clear during communications, a remote attacker could determine the WEP key and decrypt RG-1000 traffic. Published Before: 8/2/2001 Severity: High

CAN-2001-0352: SNMP agents in 3Com AirConnect AP-4111 and Symbol 41X1 Access Point allow remote attackers to obtain the WEP encryption key by reading it from a MIB when the value should be write-only, via (1) dot11WEPDefaultKeyValue in the dot11WEPDefaultKeySTable of the IEEE 802.11b MIB, or (2) ap128bWepKeyValue in the ap128bWEPKeyTable in the Symbol MIB. Published Before: 7/21/2001 Severity: Medium

CAN-2001-0382: Computer Associates CCC\Harvest 5.0 for Windows NT/2000 uses weak encryption for passwords, which allows a remote attacker to gain privileges on the application. Published Before: 6/18/2001 Severity: High

CAN-2001-0133: The web administration interface for Interscan VirusWall 3.6.x and earlier does not use encryption, which could allow remote attackers to obtain the administrator password to sniff the administrator password via the setpasswd.cgi program or other HTTP GET requests that contain base64 encoded usernames and passwords. Published Before: 3/12/2001 Severity: High

CAN-1999-0757: The ColdFusion CFCRYPT program for encrypting CFML templates has weak encryption, allowing attackers to decrypt the templates. Published Before: 3/12/2001 Severity: Medium

CAN-2001-0103: CoffeeCup Direct and Free FTP clients use a weak encryption to store passwords in the FTPServers.ini file, which could allow attackers to easily decrypt the passwords. Published Before: 2/12/2001 Severity: Medium

CAN-2000-1173: Microsys CyberPatrol uses weak encryption (trivial encoding) for credit card numbers and uses no encryption for the remainder of the information during registration, which could allow attackers to sniff network traffic and obtain this sensitive information. Published Before: 1/9/2001 Severity: Medium

### 42.2 Brute-force attacks

Category 42.2 Brute-force attacks

2002-11-14 supercomputer cryptanalysis brute-force speed power keylength keyspace

NewsScan

#### CRAY LAUNCHES NEW LINE OF SUPERCOMPUTERS

Cray released more details about its long-awaited Cray XI machine and says it plans to begin shipping, on schedule, by the end of this year. An entry-level Cray XI will start at \$2.5 million, but CEO Jim Rottsolk says he expects the majority of systems sold to range from \$5 million to \$40 million. A top-of-the-line machine with 50 cabinets would cost \$200 million to \$300 million and would likely topple NEC's position as the maker of the world's fastest system. (Wall Street Journal 14 Nov 2002)

Category 42.2 Brute-force attacks

2002-11-15 supercomputers contest cryptanalysis brute-force factoring

NewsScan

#### SUPERFAST SUPERCOMPUTERS

And they're off and running and it's neck and neck at the turn... Or, anyway, NEC. In the current ranking of world's fastest-computers, compiled semi-annually by computer scientists at the University of Tennessee and the University of Mannheim, the fastest computer right now is the Earth Simulator, made by NEC Corporation of Japan. Of the remaining computers in the top ten, seven are from the U.S., one is from France, and one is from the United Kingdom. One of the top-ranked supercomputers, the NetworkX/Quadrics machine at Lawrence Livermore National Laboratories in California, uses the Linux operating system and Intel microprocessors. In the new ranking, the U.S. has 46% of all supercomputer systems installed, and is the producer of 91% of all systems manufactured. (New York Times 15 Nov 2002)

Category 42.2 Brute-force attacks

2002-11-19 supercomputers cryptanalysis brute-force factoring

NewsScan

#### SUN SUPERCLUSTERS

Sun Microsystems has developed new superclustering technology (code-named Wildcat) capable of achieving throughput rates of 4.8 gigabytes to one teraflop per second; now called Sun Fire Link connect, the technology will be used in data center operations in education, research, government, and other facilities. Calling it a "much more scalable cluster interconnect to address commercial and high-performance computing environments," Sun says that Fire Link will have the capability to support up to 800 CPUs. (Internet.com 18 Nov 2002)

Category 42.2 Brute-force attacks

2002-11-20 supercomputers cryptanalysis brute-force factoring

NewsScan

#### IBM COMPUTERS TO RIVAL HUMAN BRAIN

IBM has signed a \$290 million contract with the federal government for new supercomputers; one, called ASCI Purple, is eight times faster than the computer currently used for nuclear testing; the second, called Blue Gene/L, will be used in weather modeling. Blue Gene/L will be powered by 130,000 of IBM's new Power5 microprocessors and will be 400,000 times faster than the typical home computer. ASCI Purple will be 2 1/2 times faster than the current speed champion, NEC's Earth Simulator. (Reuters/Forbes Newswire 20 Nov 2002)

# 42.3 Crypto product implementation flaws

Category 42.3 Crypto product implementation flaws

2002-07-12 **PGP** plugin encryption flaw bug

NewsScan

#### PRETTY POOR PRIVACY FROM NETWORK ASSOCIATES

A computer security company has uncovered a flaw in PGP (Pretty Good Privacy) -- a freely distributed, public key encryption system that's used to scramble e-mail messages -- that could allow malicious users to unscramble sensitive messages. The flaw is found only in PGP plug-ins for Microsoft Outlook users distributed by Network Associates. "The PGP vulnerability enables an attacker to send a specially crafted e-mail to any Outlook address enabled with the PGP plug-in, which will in turn give them access to that system," says eEye Digital Security, which discovered the problem. EEye chief hacking officer Marc Maiffret says the flaw allows an attacker to do "anything a user of that machine could do -- copy files, delete files, install a backdoor." Gartner research director for Internet security John Pescatore says, "This vulnerability means people using [the affected] version of PGP actually are less secure than if they weren't using security at all. It's always a really, really bad thing when a security product has a bug." (NewsFactor Network 11 Jul 2002) http://www.ecommercetimes.com/perl/story/18560.html

Copyright © 2003 M. E. Kabay.

### 43.1 Tokens

Category 43.1 Tokens

2002-01-08 token identification authentication I&A drivers' license registration national identity

card

NewsScan

#### 'SMART' DRIVERS' LICENSES UP AHEAD

The U.S. Transportation Department is working with the states to develop a new generation of drivers' licenses that contain electronically stored information such as fingerprints or retinal scans. Privacy advocates say the move toward "smart" licenses is really a backdoor way to establish federal ID cards -- an idea that has gained popularity among government officials following the Sept. 11 terrorist attacks. "The debate after Sept. 11 showed that Americans are instinctively suspicious of a single federally issued card, but they might be more sympathetic to identifications issued by businesses or perhaps states," says Jeffrey Rosen, a law professor at George Washington University. "What you're seeing here is a sort of a hardening of the driver's license that could lead to development of a national ID system without creating a national ID card," says Marc Rotenberg, who heads up the Electronic Privacy Information Center. (AP 8 Jan 2002)

http://apnews.excite.com/article/20020108/D7GTF1H01.html

Category 43.1 Tokens

2002-02-06 smart card token consumer profiling data storage identification authentication I&A

e-commerce

NewsScan

#### NEW SMART CARD COULD KNOW EVERYTHING

A San Francisco company called PrivaSys has developed a battery-powered smart card that could be used to replace all the individual credit and debit cards a consumer might carry. The internal chip on the card will be able to store "loyalty" accounts (such as Frequent Flyer data) for a number of different vendors. The company has struck a deal with First Data, but will have to form additional alliances with other credit-processing companies to achieve its plan to make its card the only one you'll need in your purse or wallet. (USAToday 6 Feb 2002)

http://www.usatoday.com/life/cyber/tech/review/2002/2/06/smartcard.htm

Category 43.1 Tokens

2002-02-27 personal identification implanted token microchip skin transponder privacy

anonymity

NewsScan

#### CHIP ID IS ONLY SKIN-DEEP [19 Dec 2001]

Applied Digital Solutions, based in Palm Beach, Florida, is making headlines with plans to become the first company to sell microchips designed to be implanted into humans. One initial target market is likely to be people with artificial limbs and organs -- a user could have up to 60 words of relevant medical information embedded in the chips, which could then be read by medical personnel if the patient were brought unconscious into an emergency room. With rollout in South America scheduled in about 90 days, another potential market is potential kidnap targets who could use the chips in combination with GPS devices to alert security personnel to their whereabouts. Future plans call for ordinary people to use the chips as the ultimate ID, supplanting the functions now performed by passwords and keys. "I'd be shocked if within 10 years you couldn't get a chip implanted that would unlock your house, start your car and give you money," says Chris Hables Gray, author of "The Cyborg Citizen." And lest you think it unlikely that you'd want to try something like this out, futurist Paul Saffo reminds us, "As some people wring their hands about the invasion of privacy and civil liberty, a whole other generation is going to go, 'Cool! I've always wanted to embed technology in my body.' It's going to be fashion. One sure sign that teenagers will love it is if it terrifies their parents." (Los Angeles Times 19 Dec 2001)

http://www.latimes.com/technology/la-000100545dec19.story?coll=la%2Dheadlines%2Dtechnology

#### CHIP IMPLANT COMPANY SEEKS FDA APPROVAL [27 Feb 2002]

A Florida company that has developed a computer ID chip suitable for implanting in the human body has applied to the Food and Drug Administration for approval of its product. The VeriChip, as it's called, can be used to store information, such as medical records, which could be accessed by emergency medical personnel in the event of an accident. Applied Digital Solutions says it plans to limit its marketing of the VeriChip to companies that ensure its human use voluntary. A person or intermediary company would buy the chip for about \$200 and have it encoded with the desired information. The person seeking the implant would then take the chip -- about the size of a grain of rice -- to a doctor, who would insert it under the skin with a large needle device. Meanwhile, privacy advocates have expressed doubts about the VeriChip: "The problem is that you always have to think about what the device will be used for tomorrow. It's what we call function creep. At first a device is used for applications we all agree are good but then it slowly is used for more than it was intended," says Lee Tien, an attorney for the Electronic Frontier Foundation. (AP Feb 27 2002)

http://apnews.excite.com/article/20020227/D7HUDV3O0.html

Category 43.1 Tokens

2002-03-21 identification and authentication I&A terrorism national security

Technology Review http://www.technologyreview.com/articles/garfinkel0402.asp

Simson Garfinkel wrote a penetrating analysis of the tenuous link between I&A (identification and authentication) and national security. The driver's license has become a \_de facto\_ form of I&A, used by banks, airlines, bars and innumerable other organizations. Various state governments and non-governmental groups have proposed adding biometric authentication to the usual picture. But Garfinkel concludes his analysis with the following sensible comments: "Like the FBI, which tucked a laundry list of new powers into the USA Patriot Act of 2001, the American Association of Motor Vehicle Administrators and the Department of Transportation are using the terrorist attacks as a convenient excuse for deploying a national identification system that would have been politically untenable this time last year. Remember, even if the September 11 terrorists had been carrying smart-card-enabled driver's licenses with biometric authenticators, they still would have been allowed to board their flights. American Airlines knew Richard Reid's identity-it just didn't know that he had plastic explosives concealed in his shoes. Forcing every American to carry a new state-issued identification card may cut down on illicit drinking and make things easier for police at traffic stops, but it is simply not a rational way to deal with the specter of terrorism. Better identification systems won't do much to stop people who have evil in their hearts but not in their history."

Category 43.1 Tokens

2002-03-29 homeland security identification authentication I&A biometrics smart cards airports

NewsScan

#### 'SMART CARD' FOR FREQUENT FLIERS

EDS, Maximus, and other high-tech companies are racing to capture the emerging market for "smart cards" that will allow frequent fliers to speed through air security checkpoints after they submit to retina or hand scans. Promoters of the systems believe that "trusted traveler" programs like these not only add to customer convenience but also enhance security, by providing (in the words of an EDS executive) "better knowledge of the people getting on the airplane." Civil libertarians are skeptical, and Barry Steinhardt of the American Civil Liberties Union worries that the use of such systems would "encourage security personnel to put their guard down" and that terrorists would just obtain phony documents. But Rachel Rowland of Maximus says, "It's far easier for someone to get a fake driver's license. With these cards, nobody else is going to have the same digital map of your fingerprint." (AP/San Jose Mercury News 28 Mar 2002) http://www.siliconvalley.com/mld/siliconvalley/2955860.htm

Category 43.1 Tokens

2002-04-09 homeland security terrorism I&A identification authentication identity cards

travelers airports

NewsScan

#### CAN YOU TRUST A "TRUSTED TRAVELER"?

One proposal for improving airport security has been the creation of hard-to-counterfeit "trusted traveler" ID cards for frequent travelers, but software developer Richard P. Eastman asks the obvious question: "What makes a trusted traveler? The guy who travels all the time; who travels on business; who has a reason to travel. Does that mean the terrorist can't penetrate that group? Of course he can." Beyond objections of that sort, civil libertarians have been arguing that ID cards for travelers will set a dangerous precedent. Barry S. Steinhardt of the American Civil Liberties Union predicts, "Quickly enough, policy makers are going to say, 'If this works, let's require everyone to go through background checks before they get on a plane." (New York Times 9 Apr 2002)

http://www.nytimes.com/2002/04/09/technology/09PASS.html

Category 43.1 Tokens

2002-08-09 **I&A** identification authentication wireless card surveillance monitoring

NewsScan

#### WIRELESS SECURITY SYSTEM FOR AIRPORT RAMP AREAS

The new federal Transportation Security Agency is giving \$1 million in R&D funds to the Hackensack, NJ company ID Systems, to determine whether a wireless surveillance-and-control system designed for tracking vehicles in car factories can be adapted for airports. "You can't have an airline employee walk around with 200 keys, for all the 200 vehicles," says the head of ID Systems -- so the company has developed a vehicle control system called Wireless Asset Net. To use an airport vehicle on the tarmac, an employee would have to enter an ID card into a reader to obtain authorization from a central computer. (New York Times 8 Aug 2002)

http://www.nytimes.com/2002/08/08/technology/08SECU.htm

Category 43.1 Tokens

2002-10-17 **I&A** identification authentication e-commerce token

NewsScan

#### QUIZID TARGETS DIGITAL AUTHENTICATION

U.K. firm Quizid Technologies has launched a credit-card-sized device that is being heralded as a major breakthrough in the search for greater security for Internet-based transactions. Users are issued a card and a personal code, based on a set of color keys on the card. Each time the user wants to complete a transaction, he or she punches in the color code and a random number is generated. The card works in conjunction with the Quizid vault -- a bank of computers that can process 600 authentications per second. Security experts welcomed the new device: "Without an architecture of trust more sophisticated than a PIN or password, the U.K. is definitely not in danger of becoming a first-world knowledge-based economy," says security analyst Simon Moores. (BBC News 17 Oct 2002)

http://news.bbc.co.uk/1/hi/technology/2334491.stm

Category 43.1 Tokens

2002-10-23 implantable radio wireless transponder chip identification authentication I&A

#### NewsScan

#### FDA APPROVES IMPLANTABLE ID CHIP

In a surprise move, the Food and Drug Administration okayed the use of implantable ID chips in humans, providing they are used for "security, financial and personal identification or safety applications." The FDA has still not ruled on whether the VeriChip, made by Applied Digital Solutions, can be used for medical purposes, however. The company has promoted the device in the U.S. for its ability to provide detailed medical history data in cases where the patient is unable to communicate with emergency room personnel. Applied Digital president Scott Silverman says he's happy with the FDA's decision: "We'll now go into high gear with our sales, marketing and distribution plans in the U.S.," adding that the company will focus on the security and ID aspects of the chip, at least for the time being. Meanwhile, Leslie Jacobs, whose family volunteered to "get chipped" last May, says she's still hoping the FDA will approve the VeriChip for medical use. Both her husband and son have ongoing health problems. (Wired.com 23 Oct 2002)

http://www.wired.com/news/politics/0,1283,55952,00.html

## 43.2 Biometrics

Category 43.2 Biometrics

2002-01-03 biometric face recognition identification authentication surveillance screening

NewsScan

#### DIGITAL PHOTO DATABASE TO CONFIRM IDENTITY OF FOREIGN TRAVELERS

The U.S. State Department will soon begin comparing foreign travelers' faces with digitized photographs to confirm that individuals shown in their travel papers are the same persons who actually applied and were approved for admission to this country. And new legislation being considered in Congress would require biometric identifiers on passports issued by a number of countries, including Japan and most of Western Europe, that are in the visa-waiver program. (San Jose Mercury News 3 Jan 2002)

http://www.siliconvalley.com/docs/news/svfront/026914.htm

Category 43.2 Biometrics

2002-01-19 biometrics database linkage privacy

RISKS 21 87

Ben Rosengart noted the following:

>\*Time Magazine\* is reporting that the federal Department of Transportation, by instruction of the Congress, is working to link together the states' driver databases, and also to introduce biometric security on drivers' licenses.

http://www.time.com/time/nation/article/0,8599,191857,00.html

RISKS include false arrest due to database screwups, abuse for personal reasons by government personnel, abuse by the government itself, all the RISKS known to be associated with biometrics, disclosure of the databases to the public, and probably much, much more.

Category 43.2 Biometrics

2002-01-20 **I&A** identification authentication biometrics face recognition anti-terrorist homeland security airport

nomerand security amport

Security Wire Digest 4 5

#### PALM BEACH AIRPORT PILOTS NEW BIOMETRICS PROGRAM

Palm Beach International Airport is scheduled this week to begin a 90-day pilot program that scans passengers' faces and then compares the images to a database of the country's most wanted criminals. Using technology by Miami-based ACT Systems Integrators, the program uses facial recognition technology to flag suspected terrorists, and has the capacity to compare images with up to 30,000 photographs of known criminals. If a match isn't found, the passenger's image is discarded. The American Civil Liberties Union is against the measure, believing it too intrusive and saying it violates individuals' right to privacy. The airport already uses biometrics for new employees, who must undergo fingerprint scans that are compared to a FBI database of known offenders. Current employees also will undergo the facial scanning.

Category 43.2 Biometrics

2002-01-25 biometric face recognition I&A identification authentication airport security

RISKS 21 89

Iceland's main airport will have face recognition systems installed. Chris Leeson notes in RISKS that this can work only for known faces and he hopes that the security staff will not come to rely mainly on the system.

Category 43.2 Biometrics

2002-02-18 token smart card identification authentication I&A immigration government

identity thumbprint fingerprint recognition biometrics

NewsScan

#### HONG KONG TO USE DIGITAL ID CARDS

Hong Kong is planning to introduce an identity card with an embedded digital chip containing a replica of the cardholder's thumbprint, for matching against an optical reader at border crossings into China. "You don't have to have an immigration officer there to look at the card," says an immigration official in Hong Kong. "It's just a self-service kiosk." Besides verification of identity, the chip could be made to include medical, financial, and other data on an individual, but at least for now the card will contain only basic information. Sin Chung-kai, a pro-democracy member of the Hong Kong legislature, says: "We're not opposed to people having to carry ID cards. The crux of the controversy is how much information should be stored on the card... If I were a film star and I had some kind of disease, I wouldn't want it to be on my ID card. I also wouldn't want the ID to be my cash card. I don't want my spending traced." (New York Times 18 Feb 2002) http://www.nytimes.com/2002/02/18/technology/18KONG.html

Category 43.2 Biometrics

2002-05-17 biometric authentication I&A identification fraud simulation fingerprint

NewsScan

#### 'GUMMY' FINGERS FOOL FINGERPRINT SECURITY SYSTEMS

A Japanese engineering professor has managed to trick biometric security systems using artificial fingers made with gelatin. In addition to creating a fingerprint by pushing a finger into a malleable plastic mixed with gelatin, the researchers were able to create credible fingers using fingerprints lifted from a glass. First, the latent print was hardened, using glue that sticks to the ridges of the fingerprint. The hardened print was then photographed, using a digital camera, and enhanced using Adobe Photoshop software to create heightened contrast between the ridges and gaps. The image was then transferred to a photosensitive sheet, etched into copper and used to create another mold. Both methods resulted in a fake finger that was able to fool a variety of biometric readers 80% of the time. Security experts say the experiments cast serious doubt on any claims that this type of biometric system can be made fully secure. (BBC News 17 May 2002) http://news.bbc.co.uk/hi/english/sci/tech/newsid\_1991000/1991517.stm

Category 43.2 Biometrics

2002-05-20 biometric I&A identification authentication fake fraud simulation

Security Wire Digest, Crypto-Gram

4 39

#### \*BIOMETRICS FAIL STICKY TEST

Biometrics companies found themselves in a sticky situation recently when a Japanese researcher demonstrated how a fake finger formed with gelatin fooled fingerprint readers an average 80 percent of the time. Tsumtomu Matsumoto, a graduate student at Yokohama National University, presented a study at an IT conference last week showing scanners' vulnerability. Using the same ingredients found in Gummi Bear candies, Matsumoto created a fake fingerprint modeled after an authorized user's in less than an hour. Though that method requires the user's permission, the researcher demonstrated another by lifting a legitimate user's print off a surface, digitally enhancing it on a computer and printing it on a transparent sheet. The imprint is then etched to create a fingerprint impression later filled with gelatin, which when cooled creates the same impression as the earlier gummy finger. Both types fooled 11 different detectors 70 to 90 percent of the time.

Category 43.2 Biometrics

2002-05-24 homeland security facial recognition biometrics surveillance I&A identification

authentication privacy surveillance

#### PoliTech

A press release from Visionics Corp in May 2002 included the following description of a trial of their facial recognition equipment:

>Visionics Corporation (Nasdaq: VSNX), the worldwide leader in identification technologies and systems, announced today that its latest FaceIt® ARGUS surveillance system will be used to augment security measures at the Battery Park Screening Facility in the ferry embarkation area to Ellis Island and the Statue of Liberty in the New York harbor during this Memorial Day holiday weekend.

The state of the art system is on loan from Visionics to the United States Park Police for the holiday weekend and is part of a series of stepped up security measures that will be visible at New York City landmarks.

Major Thomas H. Wilkins of the United States Park Police commented, "Since the tragic events of September 11, our agency has been focused on preventing future attacks while ensuring everyday life remains as uninterrupted as possible. Ellis Island and the Statue of Liberty are potent symbols of our country's freedoms and it is our mission to make these landmarks safe for visitors and tourists."

The installation of FaceIt® ARGUS at Battery Park Screening Facility will encompass the security portal area that precedes the ferry boarding planks. The system will automatically scan all faces passing through the entryway and compare them against a database of known terrorists compiled by federal authorities. The installation will be in compliance with Visionics' privacy principles---signage informing the public that the system is in use is posted in corresponding areas and all non-matches are automatically deleted from the system.<

Category 43.2 Biometrics

2002-05-27 I&A identification authentication biometrics facial recognition airport homeland

security

RISKS 22 10

Peter G. Neumann summarized an experimental failure:

The face recognition system in experimental use at Palm Beach International Airport on 15 volunteers and a database of 250 snapshots. The success rate is less than 50%. Extrapolations also suggest a false-positive rate of about 50 passengers a day for a single checkpoint handling 5,000 passengers. "Eyeglasses gave the system a great deal of difficulty, in spite of copious Visionics marketing hype denying this particular glitch. Small rotations of the head, fifteen to thirty degrees off the camera's focal point, also bamboozled it repeatedly, and the lighting had to be just right."

http://www.theregister.co.uk/content/55/25444.html

Category 43.2 Biometrics

2002-05-30 facial recognition biometrics I&A identification authentication civil liberties

surveillance privacy

#### NewsScan

#### ACLU BLASTS USE OF FACE RECOGNITION SYSTEMS

The American Civil Liberties Union (ACLU) has issued a stinging criticism of the use of computer-based face recognition systems to aid in the war against terrorism. ACLU official Barry Steindardt says: "To have such a system in place near the Statue of Liberty -- our nation's beacon of liberty -- is both ironic and disheartening. It may be a good sales stunt for the manufacturer, but it is an insult to the American people and to those in law enforcement who truly know how to keep us safe." The ACLU's position is that the system has a high rate of "false positives" that wrongly match people with photos of others, thereby subjecting people to "being pulled aside for intrusive searches and security checks." (ACLU 24 May 2002) http://www.aclu.org/news/2002/n052402a.html

Category 43.2 Biometrics

2002-07-25 biometric identification authentication I&A shopping

NewsScan

#### ONE-FINGER CHECKOUT AT GROCERY STORES

At various locations around the country grocery store chains are testing new technology that allows shoppers to pay for purchases simply by putting a finger on a screen that records not a full fingerprint but a digital image, or template, of certain key elements of that fingerprint, such as where lines intersect or end. The encrypted information is then matched to the customer's credit card, debit card or checking account information, as well as to any frequent-shopper "loyalty" card. Shoppers so far seem to be accepting the new technology (and feel that it provides an additional level of security), but Carlene Thissen of Retail Systems Consulting fears a possible consumer backlash over privacy concerns: "Like iris scans, retinal scans or even voice recognition, when it's attached to your body like that, there might be more of a reaction." If the new finger payment technology proves itself in grocery stores, you can expect to see it eventually used by fast food chains, video rental companies, pharmacies, and airline and hotel check-in desks. (New York Times 25 Jul 2002)

Category 43.2 Biometrics

2002-07-29 biometric identification authentication I&A fingerprint hand geometry iris voice

cards

NewsScan

#### MILITARY ID GOES HIGH-TECH

The U.S. Defense Department is developing high-tech identification cards that will encode information about the bearer's fingerprints and other unique physical characteristics, such as hand shape, iris pattern, or voice print. The next-generation cards would add another level of security by requiring computer users to log in using their ID card and password and then undergo an additional biometric scan to verify their identity. Current ID cards that are used to log on to military computer systems contain a computer chip that holds the owner's name, rank and serial number. (AP 28 Jul 2002) http://apnews.excite.com/article/20020728/D7L26PGO0.htm

Category 43.2 Biometrics

2002-10-21 **I&A** identification authentication voice recognition biometrics

NewsScan

#### VOICE-AUTHENTICATION

A voice-authentication system developed the Mountain View, CA. company Vocent will be used to help Visa International verify the unique identity of employees making password changes and customers making online purchases. Vocent says that the system, which stores a person's digital voiceprint that can be accessed over the Internet, will help Visa set new standards for online or mobile voice-verification for use by thousands of Visa's member banks. A number of other companies are also developing voice recognition or authentication technology for this and other purposes. (San Jose Mercury News 21 Oct 2002)

Category 43.2 Biometrics

2002-11-06 I&A identification authentication biometrics iris scan

NewsScan

#### THE EYES HAVE IT IN NEW IDENTIFICATION SYSTEMS

Iris-recognition systems developed by Iridian Technologies of Moorestown, NJ, are being used now in Pakistan to detect Afghani refugees who have been returning multiple times for United Nations aid, straining the UN's resources. It is one of the largest real-world tests of the Iridian technology; another major test this year has been in Saudi Arabia, where the technology was used to monitor about 25,000 pilgrims making the haji, or journey to Mecca. (KRT/San Jose Mercury News 6 Nov 2002)

#### **Passwords** 43.3

Category 43.3 Passwords 2002-03-05 quality assurance QA login identification authentication I&A procedures policies **RISKS** 

Arthur Byrnes reminded us again in RISKS of the dangers of incompetent people regardless of security efforts. Twice in a single week, he saw major companies send unencrypted e-mail containing both login IDs and associated passwords along with

Duuuuhhhh.

Don't let your employees send that kind of e-mail!

Category 43.3 Passwords 2002-06-10

password userID e-mail notification design plan confidentiality vulnerability exposure

**RISKS** 22 12

The New York Times sent out new userIDs and passwords in a single cleartext e-mail message. Worse, the user ID was firstname\_lastname and the password was an existing userID from an older system where no particular effort had been made to keep the userIDs secret.

Category 43.3 Passwords 2002-06-27 password recovery management I&A identification authentication database

management loss

RISKS 22 13

Peter G. Neumann summarized an interesting case of bad-password recovery:

After the password for accessing a Norwegian history museum's database catalog for 11,000 books and manuscripts had been lost when the database's steward died, the museum established a competition to recover it. Joachim Eriksson, a Swedish game company programmer, won the race to discover the password (ladepujd, the reverse of the name of the researcher who had created the database). How he arrived at it was not disclosed. [Source: Long-lost password discovered: Norwegian history database cracked with help from the Web, By Robert Lemos, MSNBC, 11 Jun 2002]

## 43.5 Single sign-on

Category 43.5 Single sign-on

2002-04-04 SSO single signon I&A identification authentication market analysis

Yankee Group, Security Wire Digest

26

Yankee Grouop issued a market report on single-signon (SSO) systems and found significant progress throughout enterprise security and e-commerce applications. In a summary for Security Wire Digest, reporter Anne Saita wrote, "Microsoft's Passport, which got a huge boost in use once incorporated into the .Net initiative, is leading the field in the consumer SSO market with more than 3.5 billion monthly authentications worldwide. But Microsoft can expect stiff competition down the road from AOL, which simultaneously is developing its own SSO applications within an identity management system codenamed 'Magic Carpet' and funding the Liberty Alliance, a business consortium spearheaded by Sun Microsystems that will compete head to head with Passport.

Computer Associates, IBM Tivoli and Novell also have made inroads in the legacy and client-server SSO space, as have SSO vendors that intersect the Web and legacy client-server applications markets, such as RSA Security, Entrust and Protocom, according to the report. The current lock these software giants and security companies have will make it difficult for newcomers in both the consumer and enterprise markets."

# 44.1 New crypto algorithms

Category 44.1 New crypto algorithms

2002-10-04 quantum cryptography telecommunications research development progress

NewsScan

#### QUANTUM CRYPTOGRAPHY FOR SECURE GLOBAL COMMUNICATIONS

British researchers have been able to use quantum cryptography keys encoded in photons of light to communicate through air for 23 kilometers, and the expectation is that by March of next year this capability will be extended to 1000 kilometers -- far enough to reach all LEO satellites. Because any measure of a photon will alter its quantum properties, quantum cryptography guarantees that any attempt to intercept a message will be evident. (New Scientist 2 Oct 2002) http://www.newscientist.com/news/news.jsp?id=ns99992875

## 44.2 New crypto products

Category 44.2 New crypto products

2002-01-20 broadband wireless encryption

Security Wire Digest 4 5

#### CERAGON OFFERS BUILT-IN ENCRYPTION SOLUTION IN WIRELESS SYSTEM

Ceragon Networks, a provider of high-capacity broadband wireless systems for cellular operators, enterprises and communications service providers, last week introduced EncryptAir. The product encrypts data at channel rates of 155 Mbps and above and supports secure connectivity over SDH/SONET, IP and ATM network protocols.

#### http://www.ceragon.com

Category 44.2 New crypto products
2002-03-08 encryption software

NewsScan

#### NETWORK ASSOCIATES DISCONTINUES PGP

It's hard to sell something that's given away free. Networks Associates is shutting down its division responsible for marketing and supporting PGP ("Pretty Good Privacy"), the leading encryption software, because it's available free on the Web, leaving corporate users little reason to pay money for the product. Network Associates will continue support of PGP for existing customers until their contracts expire. (San Jose Meavailabilityrcury News 7 Mar 2002) http://www.siliconvalley.com/mld/siliconvalley/2814647.htm

Category 44.2 New crypto products

2002-04-22 palmtop computer VPN secure communications public key cryptosystem infrastructure PKI PKC

Security Wire Digest 4 31

#### FUNK SOFTWARE ANNOUNCES ADMITONE VPN CLIENT FOR POCKET PC

Funk Software, a developer of RADIUS/AAA and wireless LAN security solutions, last week released the beta version of AdmitOne VPN Client for Pocket PC, software that lets handheld users establish a secure connection over a wireless link to enterprise networks. According to the company, AdmitOne VPN Client for Pocket PC implements IPsec and Internet Key Exchange technologies to fully protect the privacy of data being transmitted, and prevents the known security hazards of wireless communications including wireless eavesdropping and channel hijacking. http://www.funk.com

Category 44.2 New crypto products

2002-04-22 palmtop computer identification authentication I&A encryption software

Security Wire Digest 4 31

#### KASPERSKY LAB INTRODUCES SECURITY FOR PALM OS

Kaspersky Lab, a data-security software developer, last week released Kaspersky Security for Palm OS, which it says is a full-scale defense system for handhelds and mobile devices operating on Palm OS. According to the company, the suite is comprised of two modules; one that controls access to a device using a reliable password structure on the system level and another that controls authorized access on the application level using encrypted data. http://www.viruslist.com

Category 44.2 New crypto products

2002-04-22 workstation encryption product trade-up programs

Security Wire Digest 4 31

#### COMPANIES OFFER TRADE-UP PROGRAM TO PGP USERS

Information Security Corp. (ISC), a developer of cryptographic products, and data protection software developer PC Guardian both last week announced trade-up programs for all current Pretty Good Privacy (PGP) users. Under ISC's terms, PGP users may obtain a copy of the latest version of SecretAgent 5 file encryption utility for a reduced fee. SecretAgent 5 is a multipurpose file encryption utility that allows a user to encrypt and/or digitally sign any type of file. PC Guardian's upgrade offer requires a minimum order of 200 licenses and applies to enterprises that purchased Network Associates' PGP. http://www.infoseccorp.com

http://www.pcguardian.com

Category 44.2 New crypto products

2002-04-22 palmtop encryption synchronization software

Security Wire Digest 4 31

#### CHAPURA UNVEILS CLOAK 2.0

Chapura, a provider of synchronization software for handhelds, last week introduced Cloak 2.0, encryption software designed to store, protect, retrieve and share personal information using virtually any Palm OS handheld or Windows-compatible PC. According to the company, Cloak 2.0 can share and back up Cloak accounts via secure, encrypted files. http://www.chapura.com

Category 44.2 New crypto products

2002-11-04 quantum cryptography photons fiber optics

#### NewsScan

PHOTONIC CRYPTOGRAPHY A New York-based stat-up company called MagiQ (pronounced like the word 'magic') has developed a cryptographic system in which keys to the code are sent over a fiber optic cable as a stream of photons, which if observed by an intruder would (by the principles of quantum physics) be inevitably altered and thus rendered useless to the eavesdropper. The system will be used only over dedicated fiber cables, and the biggest customer for the system will undoubtedly be the military. Forrester Research analyst Laura Koetzle says, "The Defense Department is going to care, and that's big money for a small start-up to survive on." (New York Times 4 Nov 2002)

Category 44.2 New crypto products

2002-11-13 wireless cellular mobile telephone encryption

#### NewsScan

#### ISRAEL DEVELOPS SECURE MOBILE PHONE SYSTEM FOR MILITARY

Israel's military, in cooperation with Motorola Israel Ltd., has developed a secure mobile phone system called "Mountain Rose" and expects it to be fully operational by the beginning of 2004. The system's designers say that "there are two levels of redundancy so that in the case of a real crisis the person with the device will be able to communicate." The encryption was developed by Israel's Signal Corps, and not even Motorola knows how it works. (Reuters/San Jose Mercury News 13 Nov 2002)

## 45.1 Digital signatures / certificates

Category 45.1 Digital signatures / certificates

2002-03-12 **I&A** identification authentication digital certificates software

NewsScan; http://www.siliconvalley.com/mld/siliconvalley/2839790.htm

#### SUN TO OFFER DIGITAL IDENTIFICATION SERVICE

In a continued rivalry with Microsoft, Sun Microsystems will be offering software, hardware and service to provide corporations a way to offer their employees, customers and vendors user-authentication services and single sign-on procedures to disparate applications, from any device connected to the Internet. Called the Sun Open Net Environment Platform for Network Identity, it will be competing with Microsoft's Passport service. Aberdeen Group analyst Dana Gardner says the effect of the new Sun offering will be to "prevent any one player from getting too much control." The Enterprise Edition of the offering will manage up to 10,000 identities inside a firewall, for a price starting at \$149,995; the Internet Edition will manage up to 250,000 identities outside a firewall, and is priced starting at \$999,995. (Reuters/San Jose Mercury News 11 Mar 2002)

Category 45.1 Digital signatures / certificates

2002-04-22 **I&A** identification authentication access control digital certificates

Security Wire Digest; http://www.entrust.com

4 31

#### ENTRUST LAUNCHES ENTRUST TRUEPASS 6.0

Entrust, an Internet security products and solutions provider, last week launched Entrust TruePass 6.0. According to the company, Entrust TruePass 6.0's zero-footprint software can help organizations securely verify the credentials identity of the individuals who are visiting and using their Web portal and secure the associated transactions. ActivCard, Datakey, GemPlus, Oberthur, Rainbow and Schlumberger are announcing plans to provide Entrust Ready Smart Cards that integrate with Entrust TruePass 6.0.

## 45.3 Micropayments

Category 45.3 Micropayments

2002-11-26 bandwidth metering spam file sharing copyright violations piracy swapping

NewsScan

#### HIGH-SPEED ISPs CONSIDER PUTTING ON THE BRAKES

Many of the largest high-speed ISPs are considering capping the amount of bandwidth that their subscribers can use each month in an effort to put the brakes on rampant file-swapping. "Every major broadband provider is seriously weighing pros and cons of bandwidth consumption caps," says Michael Harris, president of research firm Kinetic Strategies. Leading the way is Bell Canada, whose DSL service has already instituted caps on bandwidth use, charging subscribers about 80 cents for each extra 100 megabytes used. The concept is controversial for several reasons: it requires ISPs to set up a traffic-monitoring system for each account and it forces the subscriber to self-ration bandwidth -- a foreign concept to people accustomed to an all-you-can-eat approach to Internet use. Critics note that unwanted content, such as pop-up ads and pornographic spam, could waste subscribers' bandwidth, but Bell Canada says its policy has been a success so far. The company offers tiered levels of service allowing 2GB, 10GB and 20GB of monthly traffic, and the percentage of customers exceeding their allotment in any given month is small -- between 6% and 8%. Cable companies are eyeing the Bell Canada experiment with interest, as their subscribers in particular are adversely affected by "bandwidth hogs." Meanwhile, the president of file-swapping company Grokster dismisses the efforts, saying, "They only thing they're going to accomplish is to make their customers angry." (CNet News.com 26 Nov 2002)

#### E-payments / e-wallets 45.4

Category 45.4 E-payments / e-wallets

2002-02-20 e-payments e-wallets disaster recovery plan failure incompetent fraud losses

**RISKS** 92ff

Jeff Jonas reported in RISKS on some alarming statistics from Pay-Pal, the firm that lets subscribers exchange money by e-mail, that they had to reveal in their prospectus to comply with Securities and Exchange Commission (SEC) guidelines. Among other problems, the firm identified major damages that could occur from interruption of service, yet their disaster recovery plan seems to allow for outages of "at least several hours." In addition, the company reported serious losses due to fraud: of the "net losses of \$264.7 million from our inception, March 8, 1999, through September 30, 2001, and net losses of \$90.6 million during the nine months ended September 30, 2001, . . . . During the four months between July and October 2000, we experienced a significant fraud episode and, as a result, we incurred gross losses due to unauthorized charge-backs totaling \$5.7 million. This amount represented 64.0% of total charge-backs due to unauthorized transactions for the year ended December 31, 2000. For the year ended December 31, 2000, the amount of losses with respect to unauthorized use of bank accounts totaled \$0.3 million. The gross amount of charge-backs received through September 30, 2001 with respect to unauthorized use of credit cards for transactions that occurred during the nine months ended September 30, 2001 totaled \$3.2 million. For the nine months ended September 30, 2001, the amount of our losses with respect to unauthorized use of bank accounts totaled \$0.9 million." According to the home page at < http://www.paypal.com >, the firm had 16 million members worldwide as of June 2002.

E-payments / e-wallets Category 45.4

2002-02-28 token identification authentication I&A e-commerce wireless interception man-in-

the-middle attacks penetration confidentiality wristwatch

#### NewsScan

#### WRISTWATCHES TO TELL TIME, ORDER HAMBURGERS, PAY FOR GAS

The Timex watch company has developed some wristwatches with Speedpass technology that uses a radio frequency transponder to communicate credit or debit card information allowing customers to pay instantly in places like Exxon and Mobil gas stations and McDonald's restaurants. The watch is currently being test-marketed in Illinois. (AP/USA Today 28 Feb 2002)

http://www.usatoday.com/life/cyber/tech/review/2002/2/28/timex-speedpass.htm

E-payments / e-wallets Category 45.4

2002-03-05 system design feedback quality assurance QA

RISKS 21 93

Peter Trei contributed this item to RISKS:

A man used City Link more than 220 times without an e-tag, attracting at least \$22,000 in fines, because he did not know it had become a toll road, the Melbourne Magistrates Court was told yesterday. [...] http://theage.com.au/articles/2002/02/26/1014704951335.html

Some highways in Australia cannot be legally used without a radio tag. This poor soul hadn't updated his address with the DMV. The RISK lies in building systems which automatically rack up charges without limit, and no backup notification system. A big flashing sign saying 'E-Tag missing!' might have helped.

Category 45.4 E-payments / e-wallets

e-commerce single logon privacy confidentiality control Web e-payment e-wallet

children

NewsScan; http://partners.nytimes.com/2002/06/27/technology/27SOFT.html

#### MICROSOFT AGREES TO CHANGE "KIDS PASSPORT" SERVICE

Prodded by criticisms from a watchdog group called Children's Advertising Review Unit of the Better Business Bureau, Microsoft has agreed to make changes in the children's version of its Passport authorization service that allows computer users to sign on only once to use multiple Web sites and services. The group had complained that, despite the suggestion by Microsoft that the service was specially designed to protect children's safety and privacy online, there was nothing unique about the children's version of the software. Microsoft insists it never intended to mislead anyone, and has agree to post various statements clarifying what the software is and isn't. (New York Times 27 Jun 2002)

Category 45.4 E-payments / e-wallets

2002-07-11 privacy certificates data sharing protection credentials e-payment e-wallet industry

coalition group

NewsScan; http://partners.nytimes.com/2002/06/03/technology/03SOFT.html

#### LIBERTY ALLIANCE SEEKS LIBERTY FROM WHOM?

The 43-member Liberty Alliance -- whose membership includes American Express, AOL Time Warner, General Motors, Nokia, Sony, and United Airlines -- is sometimes suspected of being simply an anti-Microsoft coalition, because it seemed to be formed as a way of resisting Microsoft's plans to use its ".Net Passport" technology to get a lock on Internet commerce. But the Alliance denies that motivation, and has clarified its objectives. The Liberty Alliance says its main goal is to develop open technical standards to allow Web sites and companies to share data when they have customer permission to do so. Different sets of credentials will be used for different purposes (the way, by analogy, an individual's wallet might contain a driver's license, credit cards, library cards, etc.). (New York Times 3 Jun 2002)

INDUSTRY GROUP TO UNVEIL NEW WEB ID STANDARDS The Liberty Alliance, which includes companies like Sun Microsystems, AOL Time Warner, Sony, American Express, MasterCard and Bank of America, is set to unveil new standards for identity authentication that could make memorizing long lists of Web site passwords a thing of the past. The standard makes it easy to surf between various secure sites -- from e-commerce sites to online banking, for instance -- without having to repeatedly type in password information. A competing standard from Microsoft, the Passport system, currently runs on about 200 Web sites. Microsoft and Liberty Alliance members have discussed the idea of joining forces, but no deal has been struck and some Alliance members have voiced their distrust of Microsoft's motives for wanting to cooperate. Several critics, including Sun and AOL, have suggested that the software giant has a history of "breaking" competing technology standards so they don't work as well as Microsoft's. (AP/Los Angeles Times 11 Jul 2002)

# 45.5 Watermarks / digital-rights management

Category 45.5 Watermarks / digital-rights management

2002-07-17 digital TV television recording piracy intellectual property

NewsScan

#### CONGRESS TO TACKLE DIGITAL TV IN THE FALL

Rep. Billy Tauzin (R-La.), head of the House Energy and Commerce Committee, says he's drafting legislation that he hopes will resolve many of the questions surrounding digital TV. Congress has set a 2006 deadline for television broadcasters to complete switching over to digital signals, but some have dragged their feet, fearing that they could suffer the Internet-based piracy that's plagued the music industry for several years. Meanwhile electronics makers have worried that they could be forced to produce DVD players and other devices laden with so many restrictions that consumers will shun them. The two sides have been working to develop a "broadcast flag" that would allow consumers to record shows for personal use but prevent them from sharing those recordings over the Internet. "It will come down to, 'What are the rules?" says Gary Shapiro, president of the Consumer Electronics Association. Meanwhile, there are several details still to be hammered out, such as whether consumers should be able to transfer broadcast recordings to vacation home or office computers, or whether new restrictions will disable existing DVDs and other devices. (Reuters/CNN.com 16 Jul 2002)

Category 45.5 Watermarks / digital-rights management

2002-07-19 intellectual property broadcasting recording Internet radio

NewsScan

#### RECORD LABELS SEEK TO BLOCK WEBCASTING PIRACY

The Recording Industry Association of America is asking computer and electronics manufacturers to develop an "audio performance flag" similar to the "broadcast flag" technology now under development to protect digital television programs. The flag would act as a marker that would prohibit content that had been digitally recorded from an Internet radio station from being redistributed over the Internet. Internet radio is not a significant source of piracy today, in part because of its lower quality compared to CDs, but the combination of increased broadband connections and lower broadcasting costs is expected to push webcasters toward higher-fidelity feeds. RIAA senior VP Mitch Glazier called the talks "very limited, preliminary discussions." (Los Angeles Times 18 Jul 2002)

Category 45.5 Watermarks / digital-rights management

2002-09-06 Anti-Counterfeiting Amendments CDs DVDs software digital rights

NewsScan

#### SENATOR CRITICIZES COPYRIGHT BILL

Sen. George Allen (R-Va.) is pulling his support for the proposed Anticounterfeiting Amendments of 2002 because of last-minute changes made to the legislation before it came to a committee vote. The bill originally targeted large-scale operations that counterfeit "physical features" such fake Windows holograms or the special packaging used to certify software, CDs or DVDs as authentic. But the revised version covers "any feature" used to guarantee authenticity, including technology used in digital rights management. "Opening this legislation to the digital realm has caused the virtually unanimous industry support behind it to evaporate, and it has raised a host of troubling liability issues that cause substantial harm to Internet service providers," says Allen, who chairs the Senate Republican High Tech Task Force. Companies now opposing the bill include Verizon, Microsoft, Apple, eBay and Yahoo, all of whom have voiced their concern over a section that prohibits "trafficking" in or redistributing files that contain compromised digital watermarks. They fear the new language opens up ISPs to prosecution if their subscribers send such files. The revised version has "divided the community, so to speak, the industry, and went far afield from the original intent of the bill," says an Allen spokesman. The bill is set for a full Senate vote, which could come at anytime. (CNet News.com 5 Sep 2002)

http://news.com.com/2100-1023-956811.html?tag=fd\_top

Category 45.5 Watermarks / digital-rights management

2002-10-01 digital rights management watermark

NewsScan

#### LIQUID AUDIO PATENTS BOLSTER MICROSOFT MEDIA SECURITY

Microsoft has acquired patents from Liquid Audio covering at least two technologies that are aimed at security features for distributing entertainment online. One protects identifying information hidden in a watermark within a digital file, and the other enables online distributors to limit the countries or territories where their files may be delivered. These two restrictions are critical to the music and movie industries' business models, and will boost Microsoft's ability to respond to industry demands for secure online distribution. "The rights that we've acquired today we view as being important to efforts down the road with regard to DRM (digital rights management) technologies," says a Microsoft spokesman. (Los Angeles Times 1 Oct 2002)

http://makeashorterlink.com/?C57F217F1

Category 45.5 Watermarks / digital-rights management

2002-11-01 intellectual property copyright piracy copy protection prevention mechanisms

NewsScan

#### MUSIC INDUSTRY: GONNA LOCK LOCK LOCK, "TIL BROAD DAYLIGHT

Two new digital audio disk formats, Super Audio CD or DVD-Audio, are engineered to be copy-proof, using digital watermarks encoded to lock the recordings on the disks. So far, music lovers have been slow to accept copy-protected disks as just a new fact of life, but Electronic Frontier Foundation intellectual property attorney Fred von Lohmann acknowledges that "copyright owners are entitled to use whatever formats they want to use." (He also notes slyly that "if they really want to protect their content they can go back to vinyl.") The major consumer objection is the failure to label the recordings properly, so that it's clear what's being sold. GartnerG2 industry analyst P.J. McNealy says, "I don't think anybody per se is against copy-protected CDs. I think they're against no-labeled copy-protected CDs. The labels are optional at this point." (AP/San Jose Mercury News 31 Oct 2002)

Category 45.5 Watermarks / digital-rights management 2002-11-13 digital rights management lawsuit

NewsScan

#### SONY, PHILIPS HEAD GROUP TO ACQUIRE INTERTRUST

Fidelio Acquisition Co., a group that includes Sony, Philips and other investors, is acquiring InterTrust Technologies, a firm specializing in digital rights management (DRM) technology. DRM software allows copyright holders to specify and enforce rules on the usage of digital text, music, movies or other content. The \$453-million deal will "significantly accelerate the ability to ensure secure delivery of digital content and enable the development of many exciting new services for consumers and businesses," says Sony chairman and CEO Nobuyuki Idei. InterTrust is currently locked in a legal battle with Microsoft in which it alleges the software giant violated its patents and company officials have discussed damage figures in the billions of dollars. (Wall Street Journal 13 Nov 2002)

Category 45.5 Watermarks / digital-rights management

2002-12-07 intellectual property music distribution e-commerce digital rights management piracy

NewsScan

#### GATEWAY LEADS TO DIGITAL MUSIC

Gateway and Pressplay, the online music subscription service backed by Vivendi Universal and Sony, are teaming up to offer PC buyers a new line of computers already bundled with 2,000 preloaded hit songs. Buyers will receive one to three months of Pressplay's service for free, but will have to pay at least \$9.95 a month thereafter to maintain access to the songs. The goal is to make it easy for consumers to sample and buy music without going to the trouble of downloading it from the Internet for free. The preloaded music will be constrained by the digital rights management software that Pressplay uses to deter piracy, however, and users will have to spend an extra \$1 per song if they want to move the file to a portable device or copy it onto a CD. "I can't say it's the be-all, end-all distribution model that's going to make people flock to buy access to 2,000 songs," says Gartner analyst P.J. McNealy. "This is interesting, but the portability piece is more important." (Los Angeles Times 6 Dec 2002) http://shorl.com/dyprenivihoku

Category 45.5 Watermarks / digital-rights management

2002-12-23 broadcast flag copyright intellectual property copy protection

NewsScan

#### CONTENT LOCKS ON DIGITAL BROADCASTS

An ongoing policy debate has been swirling around a "broadcast flag" being promoted by the TV industry to protect copyrighted content. The flag would consist of a few bits of information accompanying a digital transmission to signify whether and under what rules the transmitted content (e.g., a movie) may be viewed and copied. Supporters of the flag insist that it will be used merely to restrict redistribution of copyrighted material to large numbers of other people, in violation of existing laws; the idea, they say, is that the flag will "keep people honest." In rebuttal, critics like Cory Doctorow of the Electronic Frontier Foundation charge: "When they say 'This keeps honest people honest,' they mean 'This keeps honest people in chains.'... It addresses a nonexistent problem with an insufficient technical measure at great expense to liberty and innovation." (AP/San Jose Mercury News 22 Dec 2002)

# 45.6 Other e-commerce security measures

Category 45.6 Other e-commerce security measures

2002-01-10 e-commerce magnetic stripes counterfeit fraud

RISKS 21 86

Tim Christman was reading an article about the magnetic-stripe cards being used as gift certificates by some retailers when he realized that they are subject to easy fraud. He wrote,

>Ideally, the purchase of a gift card would result in a database being updated to reflect the balance associated with the card's unique account number.

Some retailers are using sequential account numbers and have no provisions to protect against a thief using a mag-stripe reader/writer to re-program a stolen card or small denomination card so that it matches the account number of a larger valued card purchased by someone else. Many retailers even provide a convenient 1-800 number so that the thief, knowing many valid account numbers, can "shop" for a card of significantly greater value.

The RISK: A form of fraud, difficult to trace, involving a minimal investment in equipment by the thief. Also note that the thief only requires the ability to query the back-end database (through the toll-free number), not the ability to manipulate the records. Perhaps more ominously, the risk is angry family members who find a zero balance on their gift cards!

Christman recommended adding bar codes to the cards and adding check digits to the magnetically-encoded account numbers but not to the visible account numbers.

Category 45.6 Other e-commerce security measures

2002-05-18 anti-piracy technology copy-protected CD damage legal liability

RISKS 22 07ff

A series of interesting contributions in RISKS debated possible liability for damage caused by copy-protected music CDs that include additional data tracks designed to crash computers when the disks are inserted in CD-ROM players. Manufacturers of the protected disks are trying to prevent music piracy, but many contributors protested that playing CDs on their computers was perfectly normal and that they had never stolen any music at all. One correspondent pointed out that Apple explicitly disclaims any responsibility for damage to their systems from inserting such disks (which typically crash their computers and get stuck in the CD-ROM drive) and describes using these disks as misapplication and therefore out of warranty. Several correspondents urged class-action lawsuits against the makers of copy-protected CDs for failing to include adequate (or any) warnings about not inserting these disks into computer CD drives.

Category 45.6 Other e-commerce security measures

2002-05-21 intellectual property copyright music copy-protection CD magic marker

NewsScan; FindLaw Download This

86

#### HI-TECH CDs YIELD TO LOW-TECH FELT-TIP MARKER TRICK

Sony's elaborate "Key2Audio" CD copy-protection technology has succumbed to a decidedly low-tech felt-tip marker used to scribble around the rim of a disc. Internet postings say that tape or even a sticky note can be used to cover the security track, typically located on the disc's outer edge. The technology prevents users from playing the CDs on a computer by adding a track that contains bogus data. Because computer drives are programmed to read data files first, the PC tries to play the bogus data file over and over again and never gets to the music files elsewhere on the disc. The result is a CD that will play on standard CD players, but not on CD-ROM drives, some portable devices and even some car stereo systems. Sony has shipped more than 11 million copy-protected CDs in Europe, with the largest number going to Germany -- a market executives say is a hotbed of illegal CD-burning. (Reuters 20 May 2002)

http://www1.excite.com/home/technology/tech\_article/0,2109,237089

#### CD CRACK: MAGIC MARKER INDEED

London -- Technology buffs have cracked music publishing giant Sony Music's elaborate disc copy-protection technology with a decidedly low-tech method: scribbling around the rim of a disk with a felt-tip marker. Internet newsgroups have been circulating news of the discovery for the past week, and in typical newsgroup style, users have pilloried Sony for deploying "hitech" copy protection that can be defeated by paying a visit to a stationery store.

http://www.wired.com/news/technology/0,1282,52665,00.html

Category 45.6 Other e-commerce security measures

2002-06-06 copyright intellectual property digital content TV decoders smart cards set-top box

Security Wire Digest 4 44

#### \*MODULE FLOATED AS SOLUTION TO DIGITAL TV HACKS

Europe hopes to come up with an affordable solution to counter the upswing in hacked smart cards to decode digital television networks. As many as a third of all digital TV viewers in some European countries access subscriber services with hacked smart cards, according to a BBC news report. The solution touted by at least one vendor is a removable Conditional Access Module, which includes both a smart card for unscrambling television signals and hardware that fits into a slot on all set-top boxes. Subscribers can download "anti-hacking" updates to the box from a telephone line or replace the module itself if a hack occurs, according to SCM Microsystems CEO Robert Sneider. Previously, the only alternative was the costly replacement of the entire set-top box. An IDC analyst expressed doubt that such a generally available device will reduce hacking since crackers can access the same tools to break the new technology.

Category 45.6 Other e-commerce security measures

2002-06-20 TCPA Trusted Computing Platform Alliance surveillance privacy identification

NewsScan

#### ENCRYPTION DEBATE

Cambridge University computer scientist Ross Anderson has rekindled the computer encryption debate by expressing fierce skepticism about the motives of the Trusted Computing Platform Alliance (TCPA), an organization formed in 1999 by Compaq, HP, IBM, Microsoft and Intel. Anderson suggests the Alliance simply provides a smokescreen that allows those mainstream computer companies to create a new form of censorship by allowing manufacturers to track and identify information about the computer hardware and operating system software of individual users: "The TCPA appears likely to change the ecology of information goods and services markets so as to favor incumbents, penalize challengers, and slow down the pace of innovation and entrepreneurship." (New York Times 20 Jun 2002) http://partners.nytimes.com/2002/06/20/technology/20CODE.html

Category 45.6 Other e-commerce security measures 2002-06-28 standards security Web

NewsScan

#### SUN JOINS MICROSOFT, IBM IN TECH STANDARDS

Sun Microsystems is joining rivals Microsoft and IBM in developing the WS-Security Web Services technical standard designed to ensure Web services transactions are secure. Sun made the decision to cooperate on the standard after receiving assurances that other companies would not be charged licensing fees for the technology. (Reuters/Los Angeles Times 28 Jun 2002) http://www.latimes.com/technology/la-fi-techbrfs28.3jun

Category 45.6 Other e-commerce security measures

2002-09-11 e-commerce cigarette vending machine artificial intelligence AI verification age

adult child

NewsScan

#### CIGARETTE VENDING MACHINES GET HIGH-TECH MAKEOVER

The cigarette vending machine, which had faded into obscurity after criticism that it offered minors easy access to tobacco, is back -- this time with high-tech twist designed to discourage underage purchasing. Brown & Williamson's new machines feature a virtual reality sales clerk who talks the buyer through the process, asking customers to swipe their ID and credit card to verify they're 18 or older. If either one fails the test, the clerk delivers a stern rebuke: "I'm sorry, but I can't sell you smokes if you're under 18. Now go home before I call your mama." The company is currently testing the machines in Los Angeles and Cleveland, and plans to install them in bars, nightclubs and restaurants. (CNN.com 11 Sep 2002)

### 45.7 Sales taxes on Internet commerce

Category 45.7 Sales taxes on Internet commerce

2002-11-13 Internet e-commerce taxation government regulations standards

NewsScan

#### STATES TAKE MAJOR STEP TOWARD NET SALES TAX

More than 30 U.S. states have approved the Streamlined Sales Tax Project, giving a boost to efforts aimed at creating a system to impose state and local sales tax on items sold via the Internet. The agreement sets unified definitions of products, which previously had varied from region to region, and also requires participating state and local governments to impose only one statewide tax rate for each type of product by 2006. "This is the end of the beginning," said Frank Shafroth, head of state and federal relations at the National Governors Association. "The next step is doing the heavy lifting and getting the state legislatures to actually enact legislation." According to estimates from the Institute for State Studies, state governments could lose some \$45 billion in revenue in 2006 and \$55 billion in 2011 if online vendors continue to be exempt from collecting taxes on sales to consumers in states where the e-tailer has no physical presence. Detractors of the plan, including the Direct Marketing Association, charge that the agreement is flawed, and could double the number of tax rates to 15,000 rather than reduce them to 200, as claimed. (Reuters/CNet 12 Nov 2002) http://news.com.com/2100-1017-965554.html

## 46 Cryptography exports from US

Category 46 Cryptography exports from US

2002-01-02 EAR Export Administration Regulations loosening restrictions high technology

supercomputers

NewsScan

#### BUSH RELAXES COMPUTER EXPORT CONTROLS [2 Jan 2002]

The Bush administration has rolled back restrictions on sales of high-speed computers to Russia, China, India and some countries in the Middle East, more than doubling the allowable processor speed to 195,000 MTOPS (millions of theoretical operations per second). A typical U.S. home PC now sold in retail stores tops out at about 2,100 MTOPS. The change means that those countries will now have access to U.S. computers capable of complex 3D modeling, calculating fluid dynamics, and other advanced applications. The U.S. will maintain its high-tech embargo on exports to North Korea, Iran, Iraq, Libya, Cuba, Sudan and Syria. (Reuters 2 Jan 2002)

http://www1.excite.com/home/technology/tech\_article/0,2109,199172|technology | 01-02-2002::19:33|reuters,00.html

Category 46 Cryptography exports from US

2002-04-25 EAR US encryption expert restrictions controls homeland security infrastructure

protection

Security Wire Digest 4 32

#### \*EXPORT ADMINISTRATION OPERATES UNDER NEW NAME

To better reflect its new role in cybersecurity, the U.S. Bureau of Export Administration is now called the Bureau of Industry and Security. The agency is tasked with preventing certain technologies from being exported to countries hostile toward the United States. The bureau has assumed a more visible role in homeland security since the Sept. 11 terrorist attacks, including coordinating all U.S. Department of Commerce homeland security activities and leading an outreach program to educate private industry on critical infrastructure protections.

# Pointing, linking, deep linking, metatext

Category 4A2 Pointing, linking, deep linking, metatext

2002-05-14 deep linking copyright intellectual property Web courtesy etiquette consideration

politeness

#### PoliTech

An increasing number of firms have been suing Web site owners for daring to post the URLs of material in the originating Web sites that allow advertisement-laden pages to be bypassed. Known as deep-linking, this practice is seen by many ad-supported sites as a form of appropriation of content. Robin Miller, Editor in Chief of OSDN (Linux.com, Newsforge.com, freshmeat.net, Slashdot.org, DaveCentral.com, and other popular tech Web sites), pointed out on PoliTech that it should be a matter of simple courtesy to respect the owners' preferences by avoiding deep linking.

[MK comment: Be particularly careful not to circumvent Web publisher's wishes when they require registration to access materials such as White Papers. It's usually trivially easy to obtain the actual URL of the paper, but it would be discourteous to the people who are offering the material to distribute that URL, thus allowing their registration to be bypassed.]

Category 4A2 Pointing, linking, deep linking, metatext

2002-06-10 deep linking copyright intellectual property lawsuit Web

NewsScan

#### DANISH PUBLISHERS PROTEST DEEP LINKING

The Danish Newspaper Publishers' Association is suing a news Web site that provides links directly to news stories, without going through the site's home page. Newsbooster editor-in-chief Nicolai Lassen says linking directly to the story saves the reader time: "From the home page down to the actual story you want to read can be a very, very long way. By using a technology such as Newsbooster, you save a lot of time." Newsbooster charges users a subscription fee to send links to news items containing user-designated keywords, and the Danish Newspaper Publishers' Association believes that it should either shut down or negotiate to share those fees. "We consider it unfair to base your business upon the works of others," says the group's managing director. But to Internet purists, the whole point of Web is to create linkages between relevant pages. If the Web's creators hadn't wanted linking, "they would have called it the World Wide Straight Line," says one Web site operator. In the U.S., early court decisions have sided with deep-linking, except in cases of framing, where a site tries to make information created by other sites appear to be its own. "It was one of those issues that people thought was more or less settled. For whatever reason, these last couple of months, a spate of new disputes have come up," says an Internet legal expert. (AP 10 Jun 2002)

http://apnews.excite.com/article/20020610/D7K28Q3G0.html

Category 4A2 Pointing, linking, deep linking, metatext

2002-06-21 deep linking Web permission copyright intellectual property

Edupage

#### NPR'S LINK POLICY PROTESTED

National Public Radio has roused public protest in response to its policy on Web linking, which requires prior written consent to link to, or frame, any material on the NPR Web site. A form on the site requests the linker's name, e-mail address, physical address, phone number, information about the linking site, how long the link will remain on the site, the proposed wording, the U.S. state in which the linking site is incorporated, and whether the site is commercial. Although the permission form was updated in March 2002, the policy began to attract attention on Web logs June 19 after a blog owner posted a link to the form. NPR established the policy to support its noncommercial, journalistic nature, according to an NPR spokesman, and to track use.

Wired News, 20 June 2002

http://www.wired.com/news/business/0,1367,53355,00.html

## 4A3 Jurisdiction

Category 4A3 Jurisdiction

2002-02-27 hate speech auction censorship filtering court ruling judgement appeal international

conflict jurisdiction

NewsScan

#### NAZI MEMORABILIA CASE GETS SECOND LOOK IN U.S. COURTS [11 Feb 2002]

About a year ago a French court decided that Yahoo had violated French law by allowing French citizens to view auction sites displaying Nazi memorabilia and ruled that Yahoo pay \$13,000 a day in fines; however, in the U.S. (where the auction sites are located), a federal judge ruled that the French judgment can not be enforced in this country. That ruling is now being appealed by the two original plaintiff groups, The International League Against Racism and Anti-Semitism and the Union of French Jewish students. Alan Davidson, an attorney for the Washington, D.C.-based Internet civil liberties group Center for Democracy and Technology, warns that the French ruling "really puts free expression and communication in jeopardy on the Net," by reducing online speech to the lowest-common denominator of what is permissible as dictated by the most repressive nations. Taking a contrary point of view, University of Chicago law school professor Jack Goldsmith says that countries have the right to choose for themselves what is lawful within their own borders: "That is the essence of territorial sovereignty." (New York Times 11 Feb 2002)

http://partners.nytimes.com/2002/02/11/technology/11NECO.html?pagewanted=print

#### YAHOO FACES CRIMINAL CHARGES IN FRANCE[27 Feb 2002]

A French criminal court says it plans to prosecute Yahoo and its former president Timothy Koogle for allegedly condoning war crimes by selling Nazi memorabilia. Koogle faces a maximum sentence of five years and an approximately \$40,000 fine if found guilty -- a verdict that could have profound implications for free speech on the Net. France had ordered Yahoo in November 2000 to block French citizens from access the sites, but a U.S. federal judge ruled last fall that Yahoo, as a U.S.-based site, was not bound by French laws governing content. (Financial Times 27 Feb 2002) http://news.ft.com/news/industries/internet&e-commerce

Category 4A3 Jurisdiction

2002-11-26 jurisdiction location intellectual property copyright international

NewsScan

#### HOW DO YOU SUE A COMPANY YOU CAN'T FIND?

The Internet music-swapping firm KaZaA, which has assumed the successor role to now-defunct Napster, is being sued in a federal court in Los Angeles by the Recording Industry Association of America for copyright violations, but the RIAA has several problems to overcome. First, there is a question of geography, since KaZaA is everywhere and nowhere: its distributor, Sharman Networks, is incorporated in the South Pacific island nation of Vanuatu, it is managed from Australia, its computer servers are in Denmark, and its developers can't be found. Second, there is an issue of jurisdiction: Sharman's lawyer says, "What they're asking is for a court to export the strictures of U.S. copyright law worldwide. That's not permitted. These are questions of sovereignty that legislatures and diplomats need to decide." And third, there is the question of whether giving people the tools (KaZaA's service) to break the copyright law is itself a copyright violation, even if KaZaA itself did not misappropriate copyrighted music. (New York Times 7 Oct 2002)

#### KAZAA CASE TO DECIDE REACH OF U.S. COPYRIGHT LAW

A federal judge in Los Angeles has agreed to rule on the question whether American media companies can hold a non-U.S. Internet music file-swapping service liable for breaches of U.S. copyright law as long as a very large number of the file-swapping service's customers are in the U.S. The service in question is Kazaa, which is owned by the Austrian company Sharman Networks, and which has 21 million users. Judge Stephen Wilson has not yet decided the issue, but says he is "inclined" find that his court has jurisdiction: "I find the argument about providing the service to so many California residents compelling." An attorney for the media companies says: "This is important because it shows that you cannot escape U.S. justice by setting up shop outside the United States" -- whereas an attorney for Sharman argues that a decision to make companies liable to courts in other countries could lead to a judge "in communist China" to rule against U.S. companies that operate online. (AP 24 Nov 2002)

http://shorl.com/fahadesostigy

Category 4A3 Jurisdiction

2002-12-10 libel Internet international jurisiction lawsuit

NewsScan

#### WHERE IS THE INTERNET?

If a citizen of Country X believes he's been libeled by a magazine published in Country Y, does he sue in Country X or Country Y? Australian mining magnate Joseph Gutnick chose Australia to file his lawsuit against Dow Jones, publisher of Barron's magazine, which he alleges defamed him. Australia's highest court has just ruled that it has jurisdiction over the case, and Gutnick says that publishers will now "have to be very careful what they put on the Net. The Net is no different from a regular newspaper. You have to be careful what you write." (Reuters/San Jose Mercury News 10 Dec 2002)

Category 4A3 Jurisdiction

2002-12-16 interstate jurisdiction libel court judgement

#### NewsScan

VA. COURT THROWS OUT INTERNET LIBEL SUIT Three days after Australia's highest court ruled that an Australian businessman may sue Dow Jones & Co. for an article posted in New Jersey but accessible in Australia, a federal appeals court threw out a Virginia prison warden's lawsuit against two Connecticut newspapers, saying the articles posted on their Web sites were not aimed at a Virginia audience. The latest ruling reversed a lower court's decision that found prison warden Stanley Young could sue The Hartford Courant and The New Haven Advocate on the grounds that they falsely depicted him as racist in articles about alleged mistreatment of Connecticut inmates sent to Virginia to alleviate overcrowding. "The facts in this case establish that the newspapers' Web sites, as well as the articles in question, were aimed at a Connecticut audience," wrote Judge M. Blane Michael in the unanimous opinion. "The newspapers did not post materials on the Internet with the manifest intent of targeting Virginia readers." Both courts based their decisions on targeting, but differed in how they defined it, said Michael Geist, a professor at the University of Ottawa who tracks such rulings worldwide. "We have U.S. courts that looked largely at a commercial presence and the intended presence, while you got the Australian court more concerned about where the harm was felt." (AP 13 Dec 2002)

http://apnews.excite.com/article/20021213/D7NT6UEG0.htm

## 4A5 Archives

Category 4A5 Archives

2002-01-22 Internet Web archives legal implications lawsuit trial judgement ruling

RISKS 21 88

Roger Needham wrote in RISKS that a judge thinks that archiving news stories may violate the integrity of a criminal prosecution. "It is a principle in many jurisdictions that a jury should not know about prior charges or convictions of the accused. In a Scottish court a man was accused of a particularly revolting crime, he having been acquitted of a similar offence on a technicality a number of years ago. The judge ruled that the editor of a newspaper was in contempt of court by leaving reports of the earlier trial on line in his archive, because he had made it too easy for jurors to find out what they were not meant to know. The judge apparently believed that the greater ease of access of the on line archive as compared to a paper archive was a difference not of degree but of kind."

Category 4A5 Archives

2002-03-04 archive data loss compatibilitie media retention archives readability accessibility expiration degradation

RISKS 21 91

Chris Leeson summarized another case of technological obsolescence and data loss in archives: "The BBC's 1986 Domesday Project (a time capsule containing sound, images, video and data defining life in Britain) is now unreadable. The data was stored on 12-inch video discs that were only readable by the BBC Micro, of which only a handful still exist. The time capsule contains "250,000 place names, 25,000 maps, 50,000 pictures, 3,000 data sets and 60 minutes of moving pictures.". The article notes that the original Domesday Book (compiled in 1086 for tax purposes) is still in "mint condition."

## 4A6 Libel

Category 4A6 Libel

2002-06-21 defamation First Amendment free speech Web site contempt of court injunction

lawsuit

NewsScan

#### TO AVOID MORE JAIL TIME, ANGRY MAN SHUTS DOWN WEB SITE

After spending 111 days in jail for contempt of court, a 68-year-old Seattle man has won his release by shutting down a Web site he'd created to attack the retirement home in which he lived -- charging it violated federal housing laws, allowed neighbors to keep him up at night, and employed a manager who had a sexual dysfunction. The judge called him "a mean old man who becomes angry and vicious when he doesn't get his own way," while his lawyer was more supportive: "He had a choice between being pulling it and being put in jail by a judge who doesn't understand some of the fundamental precepts of constitutional law. He's an elderly man who doesn't need to risk his life. He can't tolerate being in solitary confinement." The man said he will continue to fight for his First Amendment rights in court. (AP/USA Today 21 Jun 2002) http://www.usatoday.com/life/cyber/tech/2002/06/21/web-jailing.htm

[Another report on this case at

 $< http://news.findlaw.com/ap/ht/1700/6-17-2002/20020617124501\_04.html >]$ 

### 4B1 Copyrights

Category 4B1 Copyrights

2002-01-08 copyright fair use intellectual property CD music DMCA amendment proposal

legislation

NewsScan

#### BILL AIMS AT PROTECTING RIGHT TO COPY DIGITAL FILES [8 Jan 2002]

Rep. Rick Boucher (D-Va.) says he will introduce legislation that would amend the Digital Millennium Copyright Act to protect consumers' right to make copies of digital files, such as songs on a CD. Boucher also has written a letter to the Recording Industry Association of America, suggesting that copy-protected CDs may violate the 1992 Audio Home Recording Act. Under that law, consumers pay a few cents extra each time they buy a blank CD, with the money going toward the recording industry to compensate them for potential losses caused by unauthorized copying. Boucher says, "I am particularly concerned that some of these technologies may prevent or inhibit consumer home recording." (Los Angeles Times 8 Jan 2002) http://www.latimes.com/technology/la-000001793jan08.story?coll=la%2Dheadlines%2Dtechnology

Category 4B1 Copyrights

2002-03-01 digital copyright protection embedded hardware legislation hearing conflict

technologists movies music

NewsScan

#### HOLLYWOOD, HIGH-TECH CLASH OVER PIRACY PROTECTION [1 Mar 2002]

The heads of several media and high-tech companies squared off yesterday before a panel of Washington lawmakers, presenting conflicting views of what should be done about digital copyright protection. The hearing was focused on legislation to be sponsored by Senate Commerce Committee Chairman Ernest Hollings (D-S.C.) that would require computer makers and consumer-electronics manufacturers to imbed copyright-protection technology in all of their products. The bill is backed by content providers, such as Walt Disney and News Corp., who accused the high-tech industry of hypocrisy in their opposition to technical safeguards for entertainment content. "They work hard to protect their own intellectual property. I would just like them to work modestly to protect the intellectual property of another industry," said Disney CEO Michael Eisner. Meanwhile, computer makers said it was unfair to place the burden of developing and installing copyright protection technology on them, warning that such technology could make it more difficult for consumers to legally record TV shows or music. "The focus in this debate needs to change from content protection to consumer protection," said Intel executive VP Leslie Vadasz. (Wall Street Journal 1 Mar 2002)

http://online.wsj.com/article/0,,SB101494577449898000.djm,00.html

Category 4B1 Copyrights

2002-03-06 intellectual property international treaty laws music piracy circumvention

encryption WIPO

NewsScan

#### DIGITAL COPYRIGHT TREATY GOES INTO EFFECT

A landmark international copyright treaty, negotiated by the World Intellectual Property Organization in 1996, takes effect today [March 6, 2002] amid controversy over whether tougher copyright rules encourage or inhibit intellectual creativity in cyberspace. A companion treaty specifically protecting digital music goes into effect in May. Both treaties outlaw attempts to circumvent encryption and other techniques used to prevent unauthorized copying and to ensure royalty payments. The treaties have been criticized by civil liberties advocates who claim the prohibitions will stymic freedom of speech on the Net, but their views have met little sympathy either in the U.S. or abroad. WIPO Director General Kamil Idris says the treaties will provide a secure platform for creators to further exploit the Internet with confidence. (Financial Times 6 Mar 2002) http://news.ft.com/news/industries/infotechnology

Category 4B1 Copyrights

2002-03-07 intellectual property e-commerce lawsuit settlement business method patent

NewsScan

#### AMAZON, BARNES & NOBLE SETTLE 1-CLICK DISPUTE

Amazon and Barnesandnoble.com have settled their long-running patent infringement lawsuit. Terms of the settlement were not disclosed. The lawsuit, filed by Amazon in 1999, alleged that Barnesandnoble.com used a customer checkout procedure that violated Amazon's patent on its "1-Click" checkout technology. The lawsuit was assailed at the time by critics who opposed "business method" patents granted for overly broad and unoriginal concepts. "Patents such as yours are the first step in vitiating the Web, in raising the barriers to entry not just for your competitors, but for the technological innovators who might otherwise come up with great new ideas that you could put to use in your own business," said technical publisher Tim O'Reilly in a letter to Amazon CEO Jeff Bezos. Bezos eventually suggested that business method patents should be limited to a three- to five-year life span, rather than the standard 20 years for patents. (Wall Street Journal 7 Mar 2002) http://online.wsj.com/article/0,sB1015466420659042800.djm,00.html (sub req'd)

Category 4B1 Copyrights

2002-03-12 intellectual property residual rights authors publishers electronic distribution e-

commerce

#### NewsScan

#### E-PUBLISHER WINS ROUND TWO IN COURT

E-publisher RosettaBooks won a second legal round against Random House when a three-judge panel unanimously upheld an earlier ruling rejecting Random House's request for a preliminary injunction against Rosetta. RosettaBooks is selling electronic versions of Kurt Vonnegut's "Cat's Cradle" and seven other old Random House titles. RosettaBooks had reached contractual agreements with the authors or their representatives regarding the rights to electronic publishing, but Random House has argued that electronic rights are not implicit because e-books are simply another version of a paper book. A RosettaBooks victory in the case would open the doors for hundreds of old titles to become available in electronic versions. (AP 11 Mar 2002)

http://apnews.excite.com/article/20020311/D7I6HQ200.html

Category 4B1 Copyrights

2002-03-22 intellectual property digital rights legislation law proposal fair use technical

standard hardware

#### NewsScan

#### HOLLINGS OFFERS BILL TO STOP ILLEGAL MUSIC AND VIDEO SHARING

Senator Ernest Hollings (D., SC) has introduced legislation that would require computermakers and Hollywood producers to agree on a technical standard that can be used to prevent computers and other devices from playing copyrighted digital files without permission. Media companies (such as Disney) favor the legislation, which protects their intellectual property, but computer and equipment companies (such as Intel) oppose it because it would restrict the functionality of new products. A Hollings aide says that the legislation respects traditional "fair use" rights for personal use. (Reuters/USA Today 22 Mar 2002) http://www.usatoday.com/life/cyber/tech/2002/03/22/digital-piracy.htm

Category 4B1 Copyrights

2002-03-29 international law copyright infringement judgement

#### NewsScan

#### KAZAA JUDGMENT OVERTURNED BY DUTCH COURT

A Dutch appeals court has ruled that KaZaA, which makes software that enables users to download music, videos and other copyrighted material, is not liable for copyright infringement. The decision overturns a judgment rendered last November, which found KaZaA guilty of violating copyright law. The appellate court ruling maintains that it's the users of KaZaA's Media Desktop software who are the infringers, and adds that Media Desktop was not exclusively designed to pirate copyrighted works. (Reuters/Los Angeles Times 29 Mar 2002)

http://www.latimes.com/technology/la-000022513mar29.story?coll=la%2Dheadlines%2Dtechnology

Category 4B1 Copyrights

2002-05-05 e-commerce advertising intellectual property consumer privacy rights

RISKS 22 05

A chorus of protest arose over comments by television industry officials who criticized viewers who skip over commercials on TV (this was in connection with the TiVo digital recording device which allows such shocking behavior). Analogies included suggestions that anyone failing to read all the advertisements in a newspaper or magazine should be prosecuted; that deep linking should be outlawed and everyone should have to start at a home page and navigate according to the Web owners' intentions; and that blocking or even ignoring pop-up ads should also be criminalized.

Category 4B1 Copyrights

2002-05-13 intellectual property copyleft copyright public access

#### NewsScan

#### A 'CREATIVE COMMONS' FOR INTELLECTUAL PROPERTY

A new nonprofit organization called "Creative Commons" is being formed by a group of law and technology scholars who want to encourage owners of intellectual property to donate some of their material to the public domain. Their first goal is to create a set of licenses that would clearly state the terms under which the public would be invited to copy a particular work and to make such works easy to identify and search for on the Web. The chairman of Creative Commons is Stanford law professor Lawrence Lessig, an intellectual property expert. (New York Times 13 May 2002) http://partners.nytimes.com/2002/05/13/technology/13FREE.html

Category 4B1 Copyrights

2002-05-21 intellectual property music license fees radio commercial non-commercial Internet

FindLaw Download This 86

WEBCASTERS SPARED EXTRA ROYALTIES

Associated Press / Wired

The Librarian of Congress has rejected proposed royalty rates that would have charged Internet broadcasters based on each Web user that listens in. Librarian James H. Billington will issue a final decision setting the new rates by June 20, the U.S. Copyright Office said Tuesday. The Copyright Office ruled in December 2000 that organizations distributing music and other radio content over the Internet must pay additional fees to record companies that hold song copyrights. In February, an arbitration panel proposed rates based on each person who is receiving a broadcast sent online. The rates ranged from .07 of a penny per song for a radio broadcast to .14 of a penny for all other copyrighted audio sent on the Internet.

http://www.wired.com/news/politics/0,1283,52691,00.html

U.S. Copyright Office

http://www.loc.gov/copyright/

Category 4B1 Copyrights

2002-05-23 TV television commercials advertising broadcasting research consumer recording

#### NewsScan

#### NETWORKS REALLY WISH YOU'D WATCH THE COMMERCIALS

A survey from NextResearch reports that 20% of the people who own digital video recorders (DVR) from TiVo or Replay TV never watch any commercials -- a finding that is scaring the advertising and broadcasting industry. Jamie Kellner of Turner Broadcasting warns that if DVR technology destroys the economics of paid advertising, the result will be the rapid expansion of pay-TV: "The free television that we've all enjoyed for so many years is based on us watching these commercials. There's no Santa Claus. If you don't watch the commercials, someone's going to have to pay for television and it's going to be you." And Daniel Jaffe of the Association of National Advertisers concurs: "You start losing marginal dollars when people who you thought you were buying are not viewing. This is not just a theoretical problem that might be happening somewhere down the line. This is happening now." What should advertisers do? Mollie Watson, a product manager for Best Buy, thinks their only hope is to do a better job and "put advertisements out there that people are actually going to choose to watch." Apparently there are such things. (New York Times 23 May 2002) http://partners.nytimes.com/2002/05/23/technology/23VIDE.html

Category 4B1 Copyrights

2002-05-28 privacy surveillance Web browsing class action lawsuit

FindLaw Download This 87

#### COMCAST SUED OVER WEB RECORDINGS

Comcast Corp., the nation's third-largest cable company, is being sued in U.S. court in Michigan over accusations it violated a federal privacy law when it recorded the Web browsing activities of each of its 1 million high-speed Internet subscribers. Lawyer Steven Goren of Bingham Farms, Mich., filed a class-action complaint against Comcast and its cable subsidiary Tuesday. Goren, who predicted "months or years" of litigation, is seeking attorney's fees plus damages of at least \$100 per day for every Comcast subscriber during the period from December to Feb. 13, when Comcast pledged to stop the practice. http://news.findlaw.com/ap/ht/1700/5-25-2002/20020525103003\_17.html

Cyberspace Privacy Resources

http://www.findlaw.com/01topics/10cyberspace/privacy/

Category 4B1 Copyrights

2002-06-07 lawsuit rights fair use copyright intellectual property advertising recording replay

NewsScan

#### IS THERE A LAW THAT SAYS YOU HAVE TO WATCH COMMERCIALS?

Surely there isn't -- says Rep. Rick Boucher (D-Va.) in his support for a consumer lawsuit seeking to confirm that users of Sonicblue's ReplayTV system have the lawful right to skip commercials when they record TV programs for later viewing. The suit has been filed in the same federal court in Los Angeles that is hearing a complaint from movie and television studios that ReplayTV allows customers to violate their copyrights, arguing that skipping commercials amounts to stealing. Sonicblue's position is: "Basically we believe that consumers have 'fair-use' rights, and everything consumers do with a ReplayTV is covered with 'fair use'." (Reuters/USA Today 6 Jun 2002)

http://www.usatoday.com/life/cyber/tech/2002/06/06/replaytv-sue.htm

Category 4B1 Copyrights

2002-06-21 intellectual property music license fees radio commercial non-commercial Internet

NewsScan

#### WEB RADIO ROYALTY RATE CUT IN HALF

Librarian of Congress James H. Billington has reduced the proposed royalty rate to be paid by Internet-only radio stations to 0.07 cents per song per listener -- half of the rate proposed by arbitrators last February. The rate now matches that proposed for traditional radio stations that also put their broadcasts on the Web. It will remain in effect only until the end of this year, when a new, as-yet-undetermined rate is supposed to take effect. The new, reduced rate came under fire from both sides, with Webcasters complaining it was still too high, and the Recording Industry Association of America arguing that it meant that "artists and record labels will subsidize the Webcasting businesses" of big Internet and radio companies, and that the fee "simply does not reflect the fair market value of the music as promised by the law." On the other side of the issue, the National Association of Broadcasters said the rate "places a prohibitive financial burden on radio-station streaming and will likely result in the termination of this fledgling service to listeners." (Wall Street Journal 21 Jun 2002) http://online.wsj.com/article/0,sB1024608353756633200.djm,00.html

EDUPAGE editors added the following information:

#### WEB RADIO FEES SET

A final schedule of fees that radio stations must pay record companies for playing music online has been released by James Billington, the Librarian of Congress. College radio stations claim that the fees are too high and will put them out of business, while the Recording Industry Association of America say they are too low and don't fairly recompense artists and recording studios. The fees are two-hundredths of a cent per listener per song for noncommercial stations and seven-hundredths of a cent for commercial radio stations. A minimum fee of \$500 per year will be assessed on all radio stations that play music online, and the fees are retroactive to October 1998, when the Digital Millennium Copyright Act took effect. (Chronicle of Higher Education, 21 June 2002)

http://chronicle.com/free/2002/06/2002062101t.htm

Category 4B1 Copyrights

2002-07-15 lawsuit Web intellectual property advertisments

NewsScan

#### PUBLISHERS SUE WEB SITE FOR MISAPPROPRIATING THEIR ADS

A group of major U.S. publishing companies, including the Washington Post Company and the New York Times Company, is suing Gator Corp., a Web site operator based in Redwood City, California, for taking ads on the publishers' Web sites and reselling them on Gator sites without authorization. The publishers say the misappropriation amounts to unfair competition with them, since Gator's competing offer to advertisers makes it harder for publishers to sell ads themselves. (Washington Post 27 Jun 2002)

http://www.washingtonpost.com/wp-dyn/articles/A52132-2002Jun26.html

#### PUBLISHERS WIN ONE AGAINST GATOR

Federal Judge Claude Hilton on Friday granted a motion for a temporary injunction that will force software firm Gator to stop displaying pop-up advertising over Web publishers' pages without permission. The ruling came in response to a lawsuit filed last month by The Washington Post, The New York Times, Dow Jones and seven other publishers, which alleges Gator's ads violate their copyrights and steal their revenue. The suit seeks a permanent injunction against Gator's ads and monetary damages for any advertising revenue derived from the publishers' Web pages. Gator develops software that manages passwords and fills out forms for about 10 million Web surfers who often download the application unwittingly through other popular file-sharing programs. Bundled in the software is a program called OfferCompanion that monitors the user's surfing habits and delivers targeted pop-up ads based on that information. For instance, if a surfer visits Toyota.com, Gator might launch a pop-up ad for Ford Motor. According to the lawsuit, Gator is "essentially a parasite on the Web that free rides on the hard work and the investments of plaintiffs and other Web site owners. In short, Gator sells advertising space on the plaintiffs' Web sites without their authorization and pockets the profits from such sales." (CNet News.com 12 Jul 2002) http://news.com.com/2100-1023-943515.html

Category 4B1 Copyrights

2002-08-06 intellectual property digital images advertising

NewsScan

#### DIGITAL ALTERATIONS IN 'SPIDER-MAN' OKAYED AS FREE SPEECH

A federal judge in New York has thrown out a lawsuit filed by billboard and building owners against Sony and other companies involved in making and distributing the movie "Spider-Man," saying that digital alterations of the billboards in Times Square for the movie are protected free speech. "What exists here is for artistic purposes a mixture of fictionally and actually depicted Times Square? this has First Amendment protection," ruled Judge Richard Owen. In the "Spider-Man" movie and trailers, ads for companies such as Cingular Wireless and USA Today were superimposed over those of Samsung and NBC. The judge also rejected claims that Sony's use of lasers to digitally film the buildings amounted to trespassing: "Light beams bounce off the plaintiff's three buildings day and night in the city that never sleeps," said Owen. The practice of altering real-life scenes for the purpose of film artistry or to satisfy marketing deals is becoming more common as digital technology makes it easy to do so. USA Today said it didn't pay for the advertising, but Cingular said it has a marketing deal with Sony tied to the film. (CNet News.com 6 Aug 2002)

http://news.com.com/2100-1023-948441.html?tag=fd\_top

Category 4B1 Copyrights

2002-08-13 copyright intellectual property control surveillance tracking court order lawsuit

injunction commercials advertisements recording swapping exchange

#### NewsScan

#### SONICBLUE WINS TEMPORARY REPRIEVE ON TV TRACKING ORDER

SONICblue, maker of the ReplayTV digital video recorder, has won a stay of a court order that would have forced it to track the television viewing habits of its customers. Movie studios, including Paramount and Walt Disney, have sued the company, saying that the recording features included in the ReplayTV devices, including the ability to skip commercials and exchange recorded programs with other users, enable users to violate studios' copyrights. Consumer advocates have objected to the court order, calling it an invasion of privacy. (Reuters 15 May 2002)

http://story.news.yahoo.com/news?tmpl=story&cid=581&ncid=581&e=4&u=/nm/20020515/tc\_nm/tech\_sonicblue\_dc\_2

#### CONSUMER SUIT SIDETRACKED IN HOLLYWOOD-VS.-REPLAYTV

A federal judge has brushed to the side legal efforts by the Electronic Frontier Foundation on behalf of five owners of ReplayTV systems who claim they are threatened by a lawsuit against SonicBlue, the Santa Clara company that makes that device. The ReplayTV 4000 system is an advanced recording device that allows watchers to make digital copies of TV shows and to skip commercials, and SonicBlue is being sued by 28 movie studios and TV networks on the grounds that the device encourages piracy and its widespread adoption would harm the industry. The Electronic Frontier Foundation and the consumers it represents argue that the decision would affect them and even make them indictable for piracy, and that they should therefore be allowed to participate in the lawsuit; however, Judge Florence-Marie Cooper says that "many, if not all" of their issues can be resolved by the trial without their direct input. (San Jose Mercury Times 12 Aug 2002)

Category 4B1 Copyrights

2002-09-05 DMCA Digital Millennium Copyright Act extension lawsuit inttellectual property

#### NewsScan

#### DUKE LAW SCHOOL TO CHALLENGE COPYRIGHT LAW EXPANSION

Duke University's law school has received an anonymous \$1 million gift earmarked for a new Center for the Study of Public Domain, which will focus on finding "the correct balance" between intellectual property rights and material that ought to be part of the public domain. Center co-director James Boyle says one target of study will be the 20-year extension of copyright duration contained in the Digital Millennium Copyright Act. Boyle says he is not a copyright abolitionist, but adds, "The burden of proof should be on those who say we need to have property rights in this situation? Why is this necessary? We see the system getting out of control, out of balance? If you want to have a rich culture an innovative society, you have to leave a large amount of material freely available for all to use." (CNet News.com 4 Sep 2002)

http://news.com.com/2100-1023-956637.html?tag=fd\_top

Category 4B1 Copyrights

2002-09-20 intellectual property music license fees radio commercial non-commercial Internet

NewsScan

#### WEB RADIO STATIONS OBJECT TO PAYING ROYALTIES

Told last month by a federal court that they would have to pay seven one-hundredths of a cent in royalties to record companies every time one of its listeners hears a copyrighted song transmitted over the Web, a group of radio stations led by the National Association of Broadcasters (NAB) and Clear Channel Communications is appealing that ruling to a higher court. The appeal challenges the right presumed right of the Copyright Office to set the royalty rates. (Bloomberg/New York Times 17 Jul 2002

#### ROYALTY FEES MAY BE THE DEATH OF INTERNET RADIO

All kinds of radio stations -- both Web-based and traditional over-the-air broadcasting stations -- have to pay copyright royalties to songwriter associations, but only the Web stations are required to pay a new performer's fee that goes to record companies. At a rate of seven-hundredths of a cent per song per listener, the fee is expected to undo the economic viability of almost all of the 10,000 Web radio stations now in existence. The 200 stations that have already ceased operations include nonprofit stations at UCLA, NYU, and other colleges and universities, and people seem to be punching different calculators to attack or defend what's going on: Congressman Rick Boucher (D, VA) is introducing a bill in support of small Webcasters and says its goal is "to make sure that Webcasters who measure their revenues in the tens of thousands are not put out of business by a copyright payment requirement in the hundreds of thousands."; using a different calculator, Hilary Rosen of the Recording Industry Association of America (RIAA) says that most college stations won't owe more than \$500 a year, and adds, "Given our problems with digital piracy on university servers, it is almost comical that they have the nerve to complain about \$500." (USA Today 21 Jul 2002)

#### WEBCASTERS LOBBY AGAINST ROYALTY ASSESSMENTS

Internet-radio proponents swarmed Capitol Hill Thursday to urge Congress to delay or lower the royalties they will have to begin paying record labels beginning Oct. 20. The webcasters have argued that the rates are too high for a new medium and are planning to appeal the rate of 0.07 cent per song per listener, which was set last June by the Librarian of Congress. The music companies are also appealing the rates, which they say are too low. The two groups are engaged in discussions in an effort to head off dueling lawsuits, but so far the talks have not produced a settlement. Some Internet radio firms and broadcasters have already shut down their webcasting operations, at least in part because of the upcoming royalty payment. "It was purely an economic decision," says the CEO of Jefferson-Pilot Corp.'s radio operations, which has stopped streaming 15 of its 17 stations online because of the fees. (Wall Street Journal 20 Sep 2002)

Category 4B1 Copyrights

2002-10-04 intellectual property copyright copying consumer rights bill proposed legislation

NewsScan

#### NEW COPYRIGHT BILL WOULD GIVE POWER TO THE PEOPLE

Rep. Rick Boucher (D-Va.) and Rep. John Doolittle (R-Calif.) have introduced legislation aimed at restoring specific fair use rights to copy digital works that were lost under the 1998 Digital Millennium Copyright Act, as well as bestowing "circumvention" rights to bypass copy protections when done "solely in furtherance of scientific research." The Digital Media Consumers Rights Act has drawn support from a broad coalition of electronics and computer interests, consumer groups and academics. "It's just time," said Consumer Electronics Association president Gary Shapiro. "Consumers have been pushed up against the ropes. This is the first time in 20 years in which consumers are going on the offense rather than on the defense." Meanwhile, entertainment groups bemoaned this latest development in the battle over digital media rights. "If this bill were to be enacted, content owners would be left with two unhappy choices: Protect their valuable works by not making them available in digital formats such as DVD, or lose all control over unauthorized reproduction and distribution," said Jack Valenti, president of the Motion Picture Association of America. The bill has no chance of passage this year, but will set the stage for debate in the next session of Congress. (Wired.com 4 Oct 2002) http://www.wired.com/news/politics/0,1283,55569,00.html

Category 4B1 Copyrights

2002-10-09 intellectual property copyright royalties fees Web radio broadcasters

NewsScan

#### COMPROMISE SOUGHT ON WEBCASTER ROYALTY FEES

Congressman F. James Sensenbrenner (R-Wisc.) is hoping that new legislation will help preserve small, independent Internet radio stations, which are threatened with insolvency because of the royalty fees imposed by a Library of Congress Copyright Arbitration Panel. The Panel had established flat fees for Web broadcasting of copyrighted music, whereas under the proposed legislation smaller stations would calculate music royalty fees as a percentage of revenue. The proposal is controversial, and an executive of Live365.com, a group of Web radio stations, says it's not much different from the current arrangement. (San Jose Mercury News 2 Oct 2002)

#### HOUSE APPROVES ROYALTY SCHEDULE FOR WEB RADIO OPERATORS

The U.S. House of Representatives has approved an arrangement that will allow smaller Web radio stations to pay a percentage of revenue or expenses (whichever is larger) rather than a flat per-song rate of .07 cents a song as was set by the Library of Congress. The deal still has to go to the Senate, but approval there seems highly likely. (Reuters/USA Today 9 Oct 2002)

Category 4B1 Copyrights

2002-10-10 copyright extension judicial review lawsuit legislation constitutionality

NewsScan

#### COURT TO REVIEW COPYRIGHT EXTENSION LAW [20 Feb 2002]

The U.S. Supreme Court announced it will review a challenge to a 1998 law that extends by 20 years the lifetime of all existing copyrights and increases the lifetime of future copyrights from 50 to 70 years after the death of the creator. The legislation, called the Sonny Bono Copyright Term Extension Act, was named after the late Sonny Bono, congressman and former entertainer. Stanford University law professor Lawrence Lessig, an attorney for one of the groups seeking to declare the legislation unconstitutional, says the case is important "so that the next Walt Disney can do to Disney what Disney did to Grimm's fairy tales" -- entirely transform material taken from the public domain. But the court likely will focus not on the substance of the law but on the issue of whether the law extends a copyright's duration far longer than what was envisioned by the framers of the Constitution. Wayne State University law professor Jessica Litman argues: "It's important for the Supreme Court to reassert that there's no copyright exception in the Constitution that Congress can do whatever it pleases. Congress has limited powers." Lawyers for the government insist that there are no legal precedents barring Congress from enacting the legislation. (Washington Post 20 Feb 2002)

http://washingtonpost.com/wp-dyn/articles/A35750-2002Feb19.html

#### COURT TO REVIEW COPYRIGHT-EXTENSION LAW [10 Oct 2002]

The U.S. Supreme Court has accepted the first copyright case in decades — a constitutional challenge to the Sony Bono Copyright Term Extension Act, which Congress passed in 1998 to extend copyright protections an additional 20 years. Under the law, creative works by an individual (such as Ernest Hemingway) are protected for 70 years after the person's death, and works by a corporation (such as the Disney Corp.) are copyright-protected for 95 years from the date of their creation. Stanford University law professor Lawrence Lessig told the court: "Just at the time that the Internet is enabling a much broader range of individuals to draw upon and develop this creative work without restraint, extensions of copyright are closing off this medium to a broad swath of our common culture." In rebuttal, the Solicitor General's position is that the issue is one that should be addressed to the legislature, not to the courts. (San Jose Mercury News 9 Oct 2002)

Category 4B1 Copyrights

2002-12-02 copyright intellectual property patents lawsuit precedent

NewsScan

#### FILE-SHARING'S FATE HANGS ON BETAMAX RULING

Like the previous lawsuits that shuttered Napster and Aimster, the latest lawsuit brought by the major record labels against peerto-peer file-swapping networks will hinge on a legal precedent set in 1984 when the Supreme Court ruled that Sony wasn't liable for copyright infringement because its Betamax VCRs had "substantial" legitimate uses as well as illegal ones. That argument proved insufficient in the earlier cases, in part because Napster and Aimster kept central directories of the files on users' computers, and were therefore in a better position to know what their users were doing. The companies now under fire --Morpheus, Kazaa and Grokster -- don't maintain any central directories, and their lawyers say that means they have no way to monitor or control what their users do. However, to bolster their case, the companies behind Morpheus, Kazaa and Grokster are now encouraging copyright owners to use file-sharing technology as a legitimate promotional or distribution tool -- for instance, by offering independent musicians the means to disseminate sample songs. In a joint brief Monday, however, the record companies indicated they're not fooled by that tactic and have reiterated their position that the companies should be held accountable for widespread piracy on their networks. "The Supreme Court in deciding the Sony case couldn't have intended to permit a massive system of infringement to be called exempt from the copyright law. It just defies reason to think otherwise," says one copyright expert. (Los Angeles Times 10 Sep 2002)

#### COURT HEARS ARGUMENTS AGAINST FILE-SWAPPING FIRMS

A federal court is scheduled to hear arguments by entertainment attorneys today, urging the judge to grant a "summary judgment" in their lawsuit against the Morpheus and Grokster file-swapping networks. The defendants have responded by asking that the case be dismissed and that they be allowed to distribute their software unmolested. If the case does go to trial, it will be the first time that any of the peer-to-peer companies have made it that far in the legal process -- Napster and Madster (formerly Aimster) fell into bankruptcy before a full trial could be held. Legal experts agree that the copyright holders' case is potentially more influential than the suit against the now-defunct Napster, and that a full trial would set an important legal precedent for the technology community. Meanwhile, the file-swapping software remains popular: according to Download.com, Morpheus was downloaded nearly 400,000 times last week and Grokster 112,000 times. Kazaa, which the entertainment groups are hoping to add to the current lawsuit, remained the most popular, with more than 3.4 million downloads last week. (CNet News.com 2 Dec 2002) http://news.com.com/2100-1023-975618.html

Category 4B1 Copyrights

2002-12-04 intellectual property e-commerce distribution licensing electronic publishing

copyright authors' rights

NewsScan

#### RANDOM HOUSE, ROSETTA END QUARREL OVER E-BOOKS

Random House has settled its lawsuit against RosettaBooks over Rosetta's sales of electronic versions of eight popular titles, including Kurt Vonnegut's "Cat's Cradle" and William Styron's "Sophie's Choice." Rosetta will continue to publish the disputed works and will work with Random House on bringing additional titles to the e-book market. "We are very glad to be able to put our differences behind us and to now work collaboratively rather than combatively to enhance RosettaBooks' and our commitment to electronic publishing," said Random House senior VP Katherine J. Trager. The case has been watched closely by other publishers, but Wednesday's settlement leaves the core issue in the lawsuit unresolved -- whether the rights to publish electronic versions of books are implied and therefore covered in contracts signed with authors in pre-Internet days. "The settlement seems neutral about rights ownership; it doesn't move things forward or back," says Paul Aiken, executive director of the Author's Guild, which represents thousands of published authors. (AP 4 Dec 2002) http://apnews.excite.com/article/20021204/D7NN77LO0.html

### 4B2 Patents

Category 4B2 Patents

2002-03-15 intellectual property patent law claim litigation judgement

NewsScan

#### U.S. JUDGE NARROWS BT PATENT CLAIM

British Telecom suffered a setback in its attempt to enforce a patent filed in the 1970s, which it says covers the concept of hyperlinking, when U.S. Judge Colleen McMahon issued an opinion that cast doubts on the relevance of some of the patent's concepts to the modern-day Internet. British Telecom is attempting to extract royalty payments from Prodigy in a first test of its ability to enforce the patent, but critics say the inventions claimed by the company were detailed in previous work by British and U.S. scientists in the 1960s and have long since entered the public domain. (Reuters 14 Mar 2002) http://story.news.yahoo.com/news?tmpl=story&cid=581&u=/nm/20020315/tc\_nm/tech\_hyperlinks\_patent\_dc\_2

Category 4B2 Patents

2002-05-28 intellectual property patent law infringement SCOTUS ruling

FindLaw Download This 87

#### PATENT PROTECTIONS UPHELD BY SUPREME COURT

A unanimous U.S. Supreme Court on Tuesday set aside a ruling on copycat products that critics have charged would have seriously undermined the protections under the nation's patent system. The justices said a U.S. appeals court was wrong in its ruling that reinterpreted a major, long-standing doctrine of patent law in a way that makes it tougher for inventors to prove patent infringement.

http://news.findlaw.com/news/s/20020528/courtpatentsdc.html

Read The Opinion (FESTO CORP. v. SHOKETSU KINZOKU KOGYO KABUSHIKI CO.)

http://laws.lp.findlaw.com/us/000/001543.html

Category 4B2 Patents

2002-06-04 fair use intellectual property digital rights copyright policy

NewsScan

#### TECHNOLOGY IS EASY, POLICY IS HARD: CERF WANTS RULE CHANGES

Internet pioneer and WorldCom senior VP Vint Cerf thinks government policies are impeding the advancement of the Internet, but acknowledges: "Policy problems are harder to solve, and probably more important than the technology ones. Policy doesn't have a simple answer. Sometimes it has to do with attitude, sometimes it has to do with culture, sometimes it has to do with the legal framework." He would like to see the government require phone and cable network companies to share those networks with Internet service providers at a fair price, and he would like to see strong support for the extension of "fair use" principles of copyright law extended to the digital world: "Even though there will be some people in the publishing industry who think fair use isn't fair, I believe it has served reasonably well. We don't have a good definition of fair use for online, digital material." If policy issues were worked out properly, technologists would be able to create a new communications environment that would have enormous impact. For example, people "could download a one-hour HDTV movie in 16 seconds. This changes your whole view of video on demand." And with new views like that will come a renaissance of communication, entertainment, and learning, because "most of the creative uses don't come from the people who design the network, they come from the people who use it. That's what happened with the World Wide Web and Java." (KRT/San Jose Mercury-News 3 Jun 2002)

http://www.siliconvalley.com/mld/siliconvalley/3392998.htm

Category 4B2 Patents

2002-06-27 intellectual property competition proprietary information codes embedded microcomputers diagnostic systems competition information warfare infowar

RISKS, http://www.cnn.com/2002/TECH/ptech/06/24/diagnosing.cars.ap/ 22 13

Monty Solomon contributed this tid-bit about the consequences of secrecy:

At least a couple of times a week, mechanic Ernie Pride tells customers at his independent repair shop he can't fix their cars because he doesn't know what's wrong with them. Go to the dealer, he advises. He has the experience and knowledge to service vehicles but lacks the closely guarded information needed to diagnose problems with today's high-tech cars. Automakers refuse to make much of it available to independent shops that compete with higher-priced dealerships. The practice is raising hackles in Congress and a vigorous defense by the industry. ... [AP, June 24, 2002]

Category 4B2 Patents

2002-07-19 intellectual patent compression algorithm images

NewsScan

#### PICTURE THIS: COMPANY CLAIMS JPEG PATENT

Forgent Networks, based in Austin, Texas, is claiming that a patent it holds covering a "coding system for reducing redundancy" directly applies to the compression technique used in the creation of JPEG images. The patent originally was granted to Compression Labs in 1986 and later acquired by Forgent, which says it will now seek licensing revenue from companies that use JPEG "in all fields of use," with the sole exception of the satellite broadcast business. Last month, Forgent sealed a licensing deal with Sony, and a company spokeswoman says it's in discussions with several other companies, but did not disclose names. In a statement published last week, Forgent said the patent could apply to companies that make "devices used to compress, store, manipulate, print or transmit digital images." The licensing plan has sparked concern among many users of digital imaging technology. "It's sort of an ambushing kind of thing," says one digital photography hobbyist. (Wired.com 19 Jul 2002)

http://www.wired.com/news/business/0,1367,53981,00.html

Category 4B2 Patents

2002-08-23 patent litigation lawsuit royalties hyperlinking Web

NewsScan

#### CLICK-AND-PAY: BT ASSERTS PATENT CLAIM FOR HYPERLINKS [7 Feb 2002]

The BT Group in the U.K. is targeting Prodigy in the first of a series of planned lawsuits aimed at enforcing its claim to have a copyright covering hypertext links. The claim, which is supported by a U.S. patent obtained in 1984 (before the creation of the World Wide Web), would allow BT to demand royalty payments from Internet service providers who offered their users the ability to surf the Web by using hyperlinks. A company spokesman argues: "We believe we have a duty to protect our intellectual property and we would expect companies to pay a reasonable royalty based on the revenues that they have enjoyed through the use of that intellectual property." Various critics of the BT lawsuit maintain that hyperlinking was conceived all the way back in the 1960s, and promoted by such well-known Internet luminaries as Ted Nelson and Doug Engelbart. (Retuers/USA Today 7 Feb 2002)

http://www.usatoday.com/life/cyber/tech/2002/02/07/patent-suit.htm

#### DOUBTS ARISE OVER BT'S CASE FOR HYPERLINK PATENT [13 Feb 2002]

Judge Colleen McMahon, the judge assigned to British Telecom's case defending its right to collect royalties from a 26-year-old patent covering hyperlinking, has raised doubts over the validity of the case. She noted that it would be difficult to prove that a patent first filed in 1976 -- long before the Web was created -- would apply to today's technology, and that comparing a 1976 computer to a 2002 computer was like comparing a mastodon with a jet. If BT prevails, its first likely target for royalty collection is Prodigy Communications, and if that attempt is successful, BT will notify other ISPs in the U.S. that they must pay up. (The U.S. is the only country where the patent has not yet expired.) Some analysts say the royalties could total tens of millions of dollars if the patent is upheld. (Financial Times 13 Feb 2002)

http://news.ft.com/news/industries/internet&e-commerce

#### BT LOSES BATTLE TO CLAIM HYPERLINK ROYALTIES

In a test case for British Telecom's claim that it owns a patent on hyperlinking technology, U.S. Judge Colleen McMahon has dismissed BT's claims, saying that Prodigy's use of the technology did not infringe on BT's 25-year-old patent. McMahon found several flaws in BT's argument, most notably that the Internet has no "central computer" as described in the original patent filing. As part of its defense, Prodigy offered a 1968 video by Stanford University computer scientist Douglas Engelbart apparently demonstrating hypertext technology, eight years before BT filed its patent application in the U.S. (BBC News 23 Aug 2002)

http://news.bbc.co.uk/1/hi/technology/2212203.stm

Category 4B2 Patents

2002-10-11 patent law court ruling appeal intellectual property

NewsScan

#### COURT RULES INTEL IN VIOLATION OF INTERGRAPH PATENTS

A U.S. federal court has concluded that Intel violated Huntsville, Alabama-based Intergraph's patents on the parallel-instruction computing (PIC) technology used in Intel's high-end 64-bit Itanium microprocessors. Intel plans to appeal. A loss will cost the company as much as \$250 million in fines and new licensing fees. (Reuters/San Jose Mercury News 11 Oct 2002)

Category 4B2 Patents

2002-11-11 patent infringement lawsuit settlement intellectual property

NewsScan

#### SONICBLUE AND TIVO CALL A TRUCE

Sonicblue and TiVo are dismissing their patent infringement claims against each other and plan to devote their energies to building the market for digital video recorders (DVRs) instead. "We believe our energies are better spent expanding the market for digital video recorders rather than fighting each other. Both sides believe in the merits of their respective positions, but the overall success of the DVR category is what is most important to the companies at this time," said the two companies in a joint statement. Sonicblue still faces a lawsuit, however, filed by major entertainment companies, including AOL Time Warner, MGM, Disney and the big three TV networks. The plaintiffs allege that the company's service, which allows viewers to strip out commercials and to send copies of recorded programs to other ReplayTV recorders via the Internet, amounts to copyright infringement. (CNet News.com 8 Nov 2002) http://news.com.com/2100-1040-965166.html

Category 4B2 Patents

2002-12-19 instant messaging patent intellectual property

NewsScan

#### AOL PATENTS INSTANT MESSAGING TECHNOLOGY AOL

Time Warner has quietly won a U.S. patent for its ICQ instant messaging technology, representing a potential goldmine for the media giant. The broadly worded patent defines AOL's IM application as one that enables users to chat with and identify one another across a specific "communications network," opening up the possibility for AOL to collect royalties from rivals. ICQ, which was developed in the mid-1990s by a group of Israeli scientists at a company called Mirabilis, was the first breakthrough chat application. It filed a patent for its technology in 1997 and was acquired by AOL in 1998 for \$287 million. (Reuters 19 Dec 2002)

## 4B3 Reverse engineering

Category 4B3 Reverse engineering

2002-04-22 intellectual property law reverse engineering chilling effect research publication

science scientists engineering engineers

Security Wire Digest 4 31

In early 2002, the IEEE began requiring authors of papers submitted to its scholarly publications to affirm that they were complying with all US laws, including the Digital Millennium Copyright Act (DMCA). In April 2002, the professional society decided to remove reference to compliance with the DMCA because so many scientists have complained that complying with this controversial law makes their normal work impossible.

Category 4B3 Reverse engineering

2002-05-21 copyright intellectual property reverse engineering DMCA prosecution trial

FindLaw Download This 86

COPYRIGHT TRIAL SET FOR RUSSIAN

Associated Press

The first criminal trial under the Digital Millennium Copyright Act will begin Aug. 26, a federal judge decided Monday. ElcomSoft Co. Ltd. of Moscow could be fined \$500,000 if convicted of selling a program that let users circumvent copyright protections on electronic-book software made by Adobe Systems Inc. Such programs are legal in Russia but banned under the 1998 Digital Millennium Copyright Act. Attorneys for the company failed this month to convince a judge that the law is too broad, vague and unconstitutional.

http://news.findlaw.com/ap/ht/1700/5-20-2002/20020520204501\_09.html

The Prosecutors

http://www.usdoj.gov/usao/can/index-2.html

Category 4B3 Reverse engineering

2002-06-06 reverse engineering encryption decryption

Security Wire Digest 4 44

#### \*STUDENT CRACKS XBOX, OPENS GAME CONSOLE TO OTHER OSES

With three weeks of work and \$50 in hardware, a graduate student at the Massachusetts Institute of Technology cracked the security protections of Microsoft's Xbox, making it possible to run competing software and operating systems on the popular video game console. In a paper posted on MIT's Web site last weekend, Andrew Huang described how he build hardware that read the Xbox's internal security system and crack the encrypted data exchanged between two chips that prevented the console from being exploited. Huang says he technique gives users the ability to turn the Xbox into a standalone computer that can run non-Microsoft software and OSes, including rival Linux. Huang says he also discovered a series of other vulnerabilities that could allow users to run the code of their choice on the box and identify users when the Xbox is connected to the Internet. http://web.mit.edu/bunnie/www/proj/anatak/AIM-2002-008.pdf

Category 4B3 Reverse engineering

2002-12-17 jurisdiction prosecution intellectual property reverse engineering e-commerce

electronic books DMCA fair use free speech

Security Wire Digest 4 26

#### \*JUDGE UPHOLDS U.S.'S RIGHT TO PROSECUTE ELCOMSOFT

A federal judge in California has ruled the United States has jurisdiction to prosecute a Russian software company that last year marketed a program on the Internet that allowed pirating of electronic books. Lawyers this week asked the same judge to dismiss copyright infringement charges leveled against ElcomSoft last year under the Digital Millennium Copyright Act (DMCA) on grounds the DMCA is too far-reaching and unconstitutional. ElcomSoft created a product that breaks the copyright protections in Adobe Systems' eBook Reader. One of its programmers, Dmitry Sklyarov, was arrested in July after speaking about the tool at the DefCon hacker conference in Las Vegas. In February, Sklyarov entered a plea-bargain deal, admitting to five DMCA violations. ElcomSoft argues the DMCA doesn't clearly define tools considered illegal, making all technologies suspect. This, they argued, violates fair-use and free speech rights. Prosecutors maintain the 1998 copyright law is broad, but clear on prohibiting tools that circumvent copyright protection controls.

#### RUSSIAN FIRM CLEARED IN U.S. COPYRIGHT CASE

ElcomSoft Co. Ltd., based in Moscow, has been found not guilty of criminal charges that it violated the 1998 U.S. Digital Millennium Copyright Act by selling a software program designed to circumvent the digital locks used to enforce copyright protections on Adobe Systems e-book software. The two-week trial was the first criminal prosecution under the controversial DCMA, which prohibits the sale of technology that can be used to break the code that "locks" digitally formatted movies, music and other software. The case hinged on whether ElcomSoft had "willfully" violated U.S. law, an intent the defendants denied. "They never intended to violate the law," said defense attorney Joseph Burton. ElcomSoft president Alexander Katalov pointed out that the program was legal in Russia and was not meant to be used for electronic books that had not been legally purchased. He said he didn't know that the software was illegal under U.S. law. (Reuters 17 Dec 2002)

# 4B4 EULA (End-user license agreements)

Category 4B4 EULA (End-user license agreements)

2002-02-08 end-user license agreement EULA lawsuit antivirus censorship contract

NewsScan

#### SOFTWARE REVIEW PROHIBITION CHALLENGED BY LAWSUIT [8 Feb 2002]

The State of New York is suing Network Associates, a company that makes McAfee Virus Scan and other software products, over a Network Associates prohibition which specifies: "The customer will not publish reviews of this product without prior consent from Network Associates Inc." New York says that the company is guilty of censoring consumers in order to shield itself "from criticism and commentary that is the essence of the free market." Network Associates argues that its use of the restriction is nothing more than an attempt by the firm to exercise its right "to set the terms of its license," which is a matter between the consumer and the company. In its response to the lawsuit, the company has also explained that its only motivation for the restriction was to make sure that customers did not publish reviews of outdated versions of products. (New York Times 8 Feb 2002)

http://partners.nytimes.com/2002/02/08/technology/08VIRU.html

### 4B5 Trademarks

Category 4B5 Trademarks

2002-04-05 intellectual property trademark proper name parody satire humor complaint

NewsScan

#### CAN FALWELL'S NAME BE TRADEMARKED TO PROTECT HIM AGAINST PARODY?

The Reverend Jerry Falwell has lodged a complaint with the World Intellectual Property Organization (WIPO) charging that a Web site that parodies him is violating his "common-law" trademark of his name. The operator of the parody Web site says Falwell's name is not entitled to trademark protection because he hasn't used it for the purpose of identifying goods and services. WIPO is headquartered in Geneva, Switzerland. (AP/San Jose Mercury News 4 Apr 2002) http://www.siliconvalley.com/mld/siliconvalley/3000509.htm

Category 4B5 Trademarks

2002-12-30 trademark infringement lawsuit

NewsScan

#### WINDOWS, LINDOWS: WHAT'S IN A NAME? A LAWSUIT

When a company focused on the Linux operating system named itself Lindows, Microsoft got mad and sued, charging that the new company had infringed on Microsoft's trademark ownership of the term Windows. Nonsense, said Lindows, and sued back, challenging the legality of that trademark. An attorney representing Lindows maintains that "no company, no matter how powerful, no matter how much money it has spent, should be able to gain a commercial monopoly on words in the English language." Funny he should mention money. Microsoft's response is that Lindows should not be allowed a "free ride on the investments we have made in building Windows into one of the most recognizable brands in the world over the last 20 years." The dispute will be decided in a Seattle courtroom in the spring. (New York Times 30 Dec 2002)

#### Paradigms, security standards 4**C**1

Category 4C1 Paradigms, security standards

2002-05-21 anonymizer bug quality assurance QA policy

NewsScan; FindLaw Download This

86

TRYING TO DENY SECURITY FLAWS 'IS ALWAYS THE WRONG ANSWER' The Web site Anonymizer.com, which offers a service that protects people's anonymity when they use the Internet, has acknowledged that it has had to fix several security flaws that had been identified by a friendly user, Bennett Haselton. Anonymizer president Lance Cottrell says that Haselton "came up with a new way of exploiting standards. They're pretty subtle." The company has awarded Haselton a prize for his effort, which is given to anyone who can find security holes in the Anonymizer service. "We are always actively soliciting people to attack it. Trying to hide and keeping your head down is always the wrong answer." (AP/San Jose Mercury News 21 May 2002)

http://www.siliconvalley.com/mld/siliconvalley/3306644.htm

#### SECURITY HOLES IN WEB PRIVACY PROGRAM

A popular Internet privacy service that lets Web surfers visit sites anonymously has fixed several serious flaws, and now the service's founder is offering a reward to the finder of the bugs. Bennett Haselton, an Internet filtering activist who runs the Peacefire Web site, found the problems with Anonymizer.com, a five-year-old service that shields users from tracking by Web sites and their Internet providers. . . Many major commercial sites cringe when security researchers find a hole. But Anonymizer actually encourages it through a "bug bounty."

http://news.findlaw.com/ap/ht/1700/5-21-2002/20020521004501\_09.html

Category 4C1 Paradigms, security standards

2002-06-06 security by obscurity open-source software homeland critical infrastructure

protection

Security Wire Digest 4 44

Edited version of an excerpt from Cheryl Balian's report in Security Wire Digest:

>A white paper released in June 2002 by the Alexis de Toqueville Institution (ADTI) in Washington, D.C., says that opensource software is inherently less secure and more likely to exploited by terrorists and other wrongdoers than closed-source, proprietary software.

The report, "Opening the Open Source Debate," suggests that the federal government's adoption of open-source software could compromise the safety of U.S. air traffic, e-commerce and surveillance systems. In a statement, ADTI says, "Terrorists trying to hack or disrupt U.S. computer networks might find it easier if the federal government attempts to switch to 'open source' as some groups propose."<

The ADTI's contention was met with incredulity by the security community, which cited Kerkhoff's principle that the security of a system should not reside in its obscurity.

## 4C2 Risk management methodology & tools

Category 4C2 Risk management methodology & tools

2002-05-23 information warfare malware subversion programmatic attacks Internet research

paper

RISKS 22 09

[Paraphrased and edited from the authors' announcement:]

Stuart Staniford, Vern Paxson, and Nicholas C. Weaver completed the paper, "How to Own the Internet in Your Spare Time" http://www.cs.berkeley.edu/~nweaver/cdc.web/ to appear in the 11th Usenix Security Symposium (Usenix Security '02).

They combined an analysis of Code Red I, the effects of Code Red II and Nimda, and the possibility of some new threats. They then use this to make a case for a CDC-like institution to proactively develop defenses for such threats.

Category 4C2 Risk management methodology & tools

2002-06-27 audit oversight independence management

RISKS 22 13

Rob Slade asked a disturbing question in a RISKS submission entitled "Qui audit ipsos auditors?"

>The Enron/Anderson debacle is fading as news, but it has some reverberations for those of us in the info tech fields.

Anderson is not alone in engaging in questionable audit practices. Others of the "Big 5" are under scrutiny, in at least two cases involving, ironically, high tech companies. For the past decade or more, there have been pressures to reduce regulatory oversight, and we are now seeing the results.

So, what is the relation to IT? Well, these are the same firms who hold the major contracts for auditing information security and assurance.

(In relation to the subject line: yes, "ISACA," I know.) <

Category 4C2 Risk management methodology & tools

2002-06-28 insurance risk statistics mandatory reporting

NewsScan

#### WHITE HOUSE WORKING TO PROMOTE CYBERSECURITY INSURANCE

The White House has been meeting with insurance industry leaders to discuss ways in which the industry could develop viable cybersecurity insurance policies for businesses. Insurance executive Robert Hartwig says, "Businesses will soon purchase this in the same way they buy property insurance. They wouldn't think of not insuring the buildings they're in, and soon they won't go without insuring the value of their computer systems." A general problem in creating such policies is that there is no real way of estimating an insurance provider's financial risk: "If you're insuring automobiles," says White House cybersecurity advisor Richard Clarke, "you can anticipate that there will be a certain number of accidents out of a given number of drivers, so you know what your loss exposure is. With cyberinsurance, there's not a lot of data that allows anyone to make that kind of prediction." (Washington Post 27 Jun 2002)

http://www.washingtonpost.com/wp-dyn/articles/A55719-20...

# 4C3 Certification of site security, privacy protection

Category 4C3 Certification of site security, privacy protection

2002-02-04 Web security certification consumer guidance

NewsScan

BETTER BUSINESS BUREAU TARGETS ONLINE PRIVACY WITH NEW SITE

The Better Business Bureau has launched a new Safe Shopping Web site that enables consumers to locate online companies that have met BBB standards for privacy in e-commerce. Visitors to

http://www.bbbonline.org/consumer/ will find nearly 11,000 Web sites that have earned one or both of the BBBOnline Privacy and Reliability seals. A recent survey showed that almost 90% of consumers would feel safer making a purchase from an online company that displays one of the seals than from a company that does not, according to Greenfield Online. "The BBB system will encourage the business community to step up to the plate and meet consumer expectations regarding online privacy," says Ken Hunter, president and CEO of the Council of Better Business Bureaus and BBBOnline. (E-Commerce Times 4 Feb 2002)

http://www.ecommercetimes.com/perl/story/16149.html

## 4C5 Industry/vendor efforts

Category 4C5 Industry/vendor efforts

2002-02-23 hardware software integration identification authentication I&A BIOS firmware

biometric fingerprint recognition digital certificate root key

#### NewsScan

#### THE MARRIAGE OF HARDWARE AND SOFTWARE SECURITY

A number of technology companies are introducing new products that embed security features inside computer hardware, to add to the protections offered by software alone. IBM and Targus Systems have developed a new biometric fingerprint reader that's built into a PC card inserted into the new IBM ThinkPad laptops, and another example of the trend is the announcement that VeriSign's "root key" software will be put into the next version of Phoenix Technology's BIOS (i.e., its basic input-output software), so that no one but an authorized user can be authenticated on the computer. (Reuters/San Jose Mercury News 23 Feb 2002)

http://www.siliconvalley.com/mld/siliconvalley/2734756.htm

Category 4C5 Industry/vendor efforts

2002-04-08 Microsoft orientation security priority policy statement features

#### NewsScan

#### MICROSOFT SAYS SECURITY IS JOB #1

In January Microsoft chairman and cofounder Bill Gates instructed the company to shift its priority from adding new software features to ensuring that its software is secure, and in the months since then the company's software designers have been reexamining the millions of lines of Windows operating system software, looking for security vulnerabilities. Rebecca Bace, a security consultant who has been critical of Microsoft, comments: "I think that the reason that people are upset with them is the perception that Microsoft will always choose the extra feature, begging the issue of whether that feature is actually of high value to the user and damning the security impact it might represent to all users." But Microsoft security expert Michael Howard insists that, if that was ever true, it's definitely not true since Gates called for a new company-wide emphasis on security as the number one priority: "Microsoft has always had a crisis-driven mentality. You have my word: we will lead the industry in delivering secure software." (New York Times 8 Apr 2002)

http://partners.nytimes.com/2002/04/08/technology/ebusiness/08SOFT.html

Category 4C5 Industry/vendor efforts

2002-04-22 management promotions publicity policy visibility

Security Wire Digest 4 31

#### \*SUN TAKES ANOTHER STEP TOWARD INCREASED SECURITY

Sun Microsystems last Thursday announced it had filled its two newly created security positions. Public key encryption inventor Whitfield Diffie was appointed chief security officer, but has been Sun's security expert since 1991. Sun also appointed Joanne Masters director of Sun's Global Security Program Office. Among her chief responsibilities are driving initiatives related to increasing Sun's presence on security issues. Sun says the positions are intended to further its development of secure information technology products and services.

http://www.sun.com/smi/Press/sunflash/2002-04/sunflash.20020417.2.html

Category 4C5 Industry/vendor efforts

2002-05-20 SSC consortium industry government security quality assurance QA reliability trustworthiness

Security Wire Digest 4 39

In mid-May 2002, Carnegie Mellon University announced the formation of the new Sustainable Software Consortium (SSC), with membership including Microsoft, Cisco Systems, Pfizer, AIG and NASA and open to other industry and government participants. Cheryl Balian wrote for Security Wire Digest, "[T]he group will research and assess computer failures, which costs U.S. companies \$100 billion per year, according to SCC research. The work of the consortium will include '...technical efforts to measure and reduce software-associated risks as well as economic, legal and policy efforts to manage risk within organizations, the broader markets and the national economy,' the group says. The SCC will also consider the feasibility of establishing widely accepted security standards for the software industry."

Category 4C5 Industry/vendor efforts

2002-05-28 homeland security biometrics surveillance privacy

NewsScan

#### SECURITY-INDUSTRIAL COMPLEX

George Washington University law professor Peter Swire calls it "a new security-industrial complex," alluding to the phrase "military-industrial complex" made famous in President Eisenhower's Farewell Address. Swire says that industry is looking at homeland security needs as a lifeline for getting out of the recession, and here are some of the many security technologies now being marketed: a variety of automatic face-recognition systems; electronic body scanners that see through clothing to detect weapons; biometric cards with embedded computer chips containing personal ID data, fingerprints, or retinal scans; databases of "trusted travelers" who could avoid long security lines at airports; and links between passenger reservation systems to other government and private databases. Privacy advocates continue to express their concerns that some of these technologies intrude too much on individual privacy. (San Jose Mercury News 27 May 2002) http://www.siliconvalley.com/mld/siliconvalley/3349627.htm

Category 4C5 Industry/vendor efforts

2002-06-27 PC security architecture announcement planning

RISKS, http://www.ntsecurity.net/Articles/Print.cfm?ArticleID=25681 22 13

From an article in NTsecurity.net:

You've heard of Trustworthy Computing, and the massive corporate remodeling going on at Microsoft where every developer, product manager, and executive assistant has been asked to rethink everything they do in the context of security. Well, that's just the tip of the iceberg. Secretly, the company has been working on a plan to rearchitect the PC from the ground up, to address the security, privacy, and intellectual property theft issues that dog the industry today. Inexplicably, the company pulled an Apple and chose to detail its plans solely to Newsweek, so we only have that one report to work from. But if Newsweek's take on the plan is correct, and consumers and businesses buy into the new devices that would result, the PC landscape will soon change forever. [...]

## 4D Funny / miscellaneous

Category 4D Funny / miscellaneous
2002-01-19 data compression advertising claims proof snake oil

RISKS 21 87

Jeremy Epstein wrote, >Snake oil is on the rise. Latest to join the fray is Zeosync (www.zeosync.com), which announced on 7 Jan 2002 that they have new algorithms that can provide 100:1 lossless data compression over "practically random" data. (What they mean by "practically" isn't defined.) Lots of criticism and proofs that it's impossible in Slashdot http://slashdot.org/article.pl?sid=02/01/08/137246&mode=thread and elsewhere. So far the algorithms haven't been given, except to provide the single longest stream of buzzwords I've seen in a long time.<

MORAL: Be skeptical of miracles using undocumented methods.

Category 4D Funny / miscellaneous
2002-01-20 Microsoft security initiative

Security Wire Digest 4

Bill Gates' announcement in January 2002 caused ripples of amazement, incredulity, approval and encouragement in the IT and security industries. Writing in a memo to employees, Gates affirmed, "When we face a choice between adding features and resolving security issues, we need to choose security. Our products should emphasize security right out of the box, and we must constantly refine and improve that security as threats evolve."

Shawna McAlearney and Anne Saita wrote in Security Wire Digest, "Gates's proclamation comes after the U.S. National Academy of Sciences (NAS) recommended that Congress create laws that punish software companies that knowingly release flawed and insecure products. The BBC last week reported the NAS Computer and Telecommunications Board suggests in a preliminary report that U.S. laws be amended to make software producers liable if their products pose a public or business risk."

Category 4D Funny / miscellaneous
2002-01-29 search engine play game bandwidth denial-of-service attack resource exploitation
saturation

#### NewsScan

#### GOOGLEWHACKING GAINS POPULARITY

Googlewhacking -- an offbeat pursuit of bored Web surfers -- is increasing in popularity and spawning its own legion of enthusiasts. The game starts by typing two unrelated words, such as colonoscopy and cockatiel, into Google's search bar, with the goal of obtaining a single result. The challenge is to find two words so disparate that only one match will occur among Google's 3 billion indexed Web pages. The idea originated with Gary Stock, who tracks the trend on his Web site (http://www.unblinking.com/heh/googlewhack.htm). "It used to be people wandered around the Web, but today people find themselves a space and stay there too much," says Stock. "To me, this is a good way to get people to learn." (CNet News.com 29 Jan 2002)

http://news.com.com/2100-1023-825602.html

Category 4D Funny / miscellaneous

2002-02-08 geek humor music rock 'n' roll logic gates circuit design

NewsScan

#### COMPUTERS AND ROCK 'N' ROLL: THAT'S WHAT IT'S ALL ABOUT

In the current issue of Computer magazine, former Intel computer architect Bob Colwell has an amusing piece on the relation between computers and rock 'n' roll, and here's a sample: "I particularly like spotting the correspondences between the arts and sciences. For example, you might not think a rock musician would understand what an inverter logic gate does, but apparently Eric Clapton does in his song 'Opposites': "Night after day, day after night./White after black, black after white./Fight after peace, peace after fight./Life after death, death after life." Colwell comments that "Clapton clearly understands that there is a time delay involved in propagating through the gate -- hence the word 'after.' When he figures out AND and OR gates, Clapton will be able to devise entire computers in his lyrics. Wait -- maybe that's what 'I Shot the Sheriff' is all about. Never could figure out why it was okay to shoot the sheriff but not the deputy. But that construction is very clearly a conjunctive logical expression (S AND NOT D -- hey, maybe that's why he needed the inverter)." To explain functional languages, Colwell analyzes the lyrics of "The Locomotion": "Ev'rybody's doin' a brand new dance now./ C'mon baby, do the locomotion.' I know you'll get to like it if you give it a chance now./ C'mon baby, do the locomotion." And vector processing? Well, what better example than "The Hokey Pokey": "You put your right foot in,/ You put your right foot in,/ And you shake it all about./ You do the Hokey-Pokey,/ And you turn yourself around./ That's what it's all about!" (IEEE Computer Feb 2002)

http://www.computer.org/computer/homepage/0202/ar/index.htm

Category 4D Funny / miscellaneous

2002-04-01 **joke** 

RISKS 22 02

Date: Mon, 01 Apr 2002 08:54:41 -0800 From: Crispin Cowan <crispin@wirex.com> Subject: Announcing Immunix SnackGuard

New Product Release: SnackGuard WireX Communications, Inc., 1 Apr 2002

[This arrived too late for the April Fool's Issue, but better late than never? (Or better never than later?) PGN]

WireX is pleased to announce the latest addition to the Immunix family of security tools: SnackGuard. SnackGuard effectively guards your favorite snacks in the break room from "snack smashing" attacks: the predations of other hungry engineers. This protection is especially vital in these trying times of unemployment, when nomadic tribes of hunter/gatherer geeks roam the halls of once mighty dot.com's in search of food and caffeine.

Following on StackGuard's "canary" defense, SnackGuard employs WireX's patent-pending "turkey" defense: when SnackGuard detects the "gobbling" noise of some turkey scarfing down your favorite pop tarts and heavily caffeinated beverages, it issues a pink slip, halting the gobbler.

While SnackGuard is effective in defending your snacks, it is not without costs. SnackGuard increases run time when you are running to catch the bus or the elevator, in that successful defense of your snacks tends to increase "programmer's butt". Excessive consumption of caffeinated beverages without intervening bathroom breaks may also induce personal "buffer overflows".

While SnackGuard is "free speech", it is not "free beer": you may modify and distribute this gag as you wish, but go buy your own brewskis.

Crispin Cowan, Ph.D., Chief Scientist, WireX Communications, Inc.

http://wirex.com Security Hardened Linux Distribution

http://immunix.org

Category 4D Funny / miscellaneous

2002-04-01 **ioke** 

RISKS 22 01

Yet another entry in the RISKS April-Fool's Day celebration:

Date: Mon, 21 Jan 2002 23:07:30 -0500

From: Gene Spafford <spaf@cerias.purdue.edu>

Subject: Surprise Settlement Evenly Splits Microsoft (unknown source)

[From SatireWire, via various intermediaries. Reprised for the occasion. PGN]

Decision Keeps Redmond from Monopolizing Massive Microsoft Patch Industry

Surprise Settlement Evenly Splits Microsoft; One Firm To Make Software, Other To Make Patches

Redmond, Wash. In a surprise settlement today with nine U.S. states, Microsoft agreed to be split into two independent companies -- one that will continue to make Microsoft operating systems, browsers, and server software, and another, potentially larger company that will make patches for Microsoft operating systems, browsers, and server software.

Critics immediately charged that the settlement -- which overrides a previous agreement with the U.S. Department of Justice -- does nothing to diminish Microsoft's standing as the world's most powerful software company. But industry analysts argued that providing patches for security holes in Microsoft programs is a major, untapped growth industry, and applauded the states for not allowing Redmond to control it.

"Just consider, Microsoft can make an operating system, such as Windows XP, and sell 200 million copies, but each one of those copies is going to need at least five patches to fix security holes, so that's 1 billion patches," said Gartner Group analyst Mitch Fershing. "That is an enormous, undeveloped market."

Microsoft employees seem to agree, as sources in Redmond described a "mad scramble" among staffers to position themselves for spots at the new company, called Patchsoft. Asked why people would want to leave Microsoft for a startup, the source said the answer was "really quite simple."

"Everyone here is asking themselves, 'Do I want to be part of the problem, or part of the solution?" he said.

But J.P. Morgan analyst Sherill Walk suspects another motive. "Considering the sheer number of patches we're talking about, I think the new company will become another monopoly, and I believe the people who've jumped ship very well know that."

"Nonsense. It's really all about consumer choice," responded Patchsoft's new co-CEOs, Bill Gates and Steve Ballmer.

But how will Patchsoft make money? Currently, Microsoft issues free patches for problems in Windows XP, SQL Server, Internet Explorer, Outlook, Windows 2000, Flight Simulator, Front Page, Windows Me, Media Player, Passport, NT Server, Windows 98, LAN Manager (for a complete list of MS software needing patches, see www.support.microsoft.com). Under the agreement, Microsoft will no longer issue patches, which Gates said explains the recent five-day outage at Microsoft's upgrade site. "That was planned," he said. "It was a test of the Microsoft No Patch Access system. Went perfectly. No one was able to download anything."

At a press conference to outline the settlement, Connecticut Attorney General Richard Blumenthal pledged to keep a close eye on Patchsoft to ensure it would not overcharge for its services. He also expressed hope that other firms would soon become Certified Microsoft Patch Developers (CMPDs) and challenge the spin-off. Asked if Patchsoft, with so many former Microsoft employees, will have an advantage over potential competitors in the Microsoft patch market, Blumenthal said the settlement prohibits collaboration.

"Patchsoft developers will not have any foreknowledge of bugs or security holes before software is released. They'll just have to be surprised," he said.

"So it will be just like it was when they were at Microsoft," he added.

One Reuters reporter, meanwhile, questioned the long-term viability of Patchsoft. "This seems like a logical split right now, but what if Microsoft's products improve to the extent that patches are needed less frequently, or perhaps not at all?" she asked.

"I'm sorry, I can only respond to serious questions," Blumenthal answered.

\_\_\_\_\_

Category 4D Funny / miscellaneous

2002-04-01 **ioke** 

RISKS 22 01

Date: Mon, 1 Apr 2002

From: Peter Neumann <risks@sri.com> Subject: Computers to Cars (unknown source)

[I have had several requests for including this item in RISKS from those who have not yet seen it, even though it has been circulating for a while. I have no idea who originally created it, but I am grateful to the author for his or her incisive observations. PGN]

For all of us who feel only the deepest love and affection for the way computers have enhanced our lives:

At a recent computer exposition (COMDEX), Bill Gates reportedly compared the computer industry with the auto industry and stated: "If General Motors had kept up with the technology like the computer industry has, we would all be driving \$25.00 cars that got 1,000 miles to the gallon."

In response to Bill's comments, GM issued a press release stating: "If General Motors had developed technology like Microsoft, we would all be driving cars with the following characteristics:

- 1. For no reason whatsoever, your car would crash twice a day.
- 2. Every time they repainted the lines in the road, you would have to buy a new car.
- 3. Occasionally your car would die on the freeway for no reason. You would have to pull over to the side of the road, close all of the windows, shut off the car, restart it, and reopen the windows before you could continue. For some reason, you would simply accept this.
- 4. Occasionally, executing a maneuver such as a left turn would cause your car to shut down and refuse to restart, in which case you would have to reinstall the engine.
- 5. Macintosh would make a car that was powered by the sun, was reliable, five times as fast and twice as easy to drive -- but would run on only five percent of the roads.
- 6. The oil, water temperature, and alternator warning lights would all be replaced by a single "General Protection Fault" warning light.
- 7. The airbag system would ask "Are you sure?" before deploying.
- 8. Occasionally, for no reason whatsoever, your car would lock you out and refuse to let you in until you simultaneously lifted the door handle, turned the key and grabbed hold of the radio antenna.
- 9. Every time GM introduced a new car, car buyers would have to learn to drive all over again because none of the controls would operate in the same manner as the old car.

wot	and operate in the same manner as the old car.
10.	You'd have to press the "Start" button to turn the engine off.

\_\_\_\_\_

Category 4D Funny / miscellaneous

2002-04-01 **ioke** 

RISKS 22 01ff

Rob Slade published a hilarious sendup of his usual book reviews, this time proposing that Bill Murray and Gene Spafford were the madcap authors of \_Hacking for Dummies\_ and adding digs at familiar security icons throughout the review:

>Date: Mon, 1 Apr 2002 07:19:57 -0800

From: "Rob, grandpa of Ryan, Trevor, Devon & Hannah" <rslade@sprint.ca> Subject: REVIEW: "Hacking for Dummies", Bill Murray III/Gene Spafford

#### BKHAKDUM.RVW 20020401

"Hacking for Dummies", William Hugh Murray III/Eugene Spafford, 1802, 076455302X, U\$21.99/C\$437.84

%A William Hugh Murray III whmurray3@spryguy.com

%A Eugene Spafford spif@serious.purdue.edu

%C 155 Divet Road, Suite 310, San Mateo, CA 94402

%D 1902

%G 076455302X

%I International Data Group (IDG Books)

%O U\$21.99/C\$411.95 415-312-0650 fax: 415-286-2740

%P 166 p.

%S for Dummies

%T "Hacking for Dummies"

As regular RISKS readers will note, I always enjoy a new addition to the "for Dummies" series. This time the imprint has outdone itself with a lighthearted romp through network naughtiness, by two of the least known, but most accomplished, practitioners of the field.

Some may question the need for such a work, but the authors maintain that they are performing a valuable service to corporations and society at large. "A vital system security penetration community is important," they state in the introduction. "It thins the herd of security practitioners. We have a moral responsibility to ensure that those who, not having the authority to fire people who insist on using Outlook, get blamed when major events happen and are forced to look for work in other fields."

In a switch from the standard format, the "Part of Tens" comes first, pointing out how to knock holes in each of the ten domains of the security common body of knowledge. This sets up a series of helpful icons used to point out specific attacks that can be mounted against each domain. (Security management attacks tend to get a bit repetitive after a while: there are only so many ways of rewording the advice to pretend to be the CEO's secretary.)

Some common and handy attacks (such as the ubiquitous brute force denial-of-service attack, featuring a sledgehammer) are listed, but there are a number of little-known tricks, like the means of attacking a computer that has been sealed in a lead-lined vault, surrounded by armed guards, and cast in concrete. Dorothy Denning's sidebar on starting wars by manipulating e-mail systems is particularly interesting. Security professionals are not ignored: in an interesting display of fair-mindedness, the authors suggest that incident-response team members prepare by ensuring they always have plenty of sugar in their gas tanks for extra energy on late-night calls.

Critical reaction to the tome has been spirited but mixed. Winn Schwartau, in the foreword, asks "is it moral, is it ethical" to provide such information to the general public, before concluding, "Who cares? Nobody has time for this." Phil Zimmermann has roundly condemned the section on anonymous communications, stating that the government has a legitimate need for access to private communications, while Fred Cohen is upset that the authors suggest viruses could be used for beneficial purposes. Richard Stallman is reported to be disturbed by the position that software development can take place in the kind of anarchic environment promoted by

the book, and has launched a campaign to ensure that everyone has valid licenses for Microsoft products. Bruce Schneier, on the other hand, points out that the information in the book presents no danger to the public. "As long as you've got a strong crypto algorithm and good technical solutions, it doesn't matter about implementation and people."

copyright Robert M. Slade, 2002 BKHAKDUM.RVW 17020401 rslade@vcn.bc.ca rslade@sprint.ca slade@victoria.tc.ca p1@canada.com http://victoria.tc.ca/techrev or http://sun.soci.niu.edu/~rslade

----

RISKS 22.02

Date: Thu, 4 Apr 2002 12:21:17 PST

From: "Peter G. Neumann" < neumann@csl.sri.com>

Subject: April Foolishness

Quite a few people have apparently gone to Amazon.com to order "Hacking For Dummies" -- a bogus (i.e., nonexistent) book reviewed by Rob Slade in RISKS-22.01. Perhaps, not surprisingly, the ISBN bears a strange resemblance to the ISBN for "S\*x for Dummies". We have to call a Slade a Slade. Perhaps his review was too subtle? Perhaps your fearless moderator needs to be more obvious in highlighting April Fools' items, besides putting it up front in the issue rather than buried in its usual end-of-the-issue position? Aw, come on! April Fool's Day is seemingly a worldwide tradition, and that's part of the fun.<

Category 4D Funny / miscellaneous

2002-04-01 joke

RISKS 22 01

On April Fools, Peter Neumann's traditional joke issue of the RISKS FORUM DIGEST published a tongue-in-cheek report on the addition of software piracy law enforcement to the duties of the Bureau of Alcohol, Tobacco and Firearms: >WASHINGTON (Reuters) - The Department of the Treasury announced today that responsibility for enforcement of new federal regulations of the software industry will fall under the jurisdiction of the Bureau of Alcohol, Tobacco and Firearms (ATF). As the regulations come into effect, the bureau will be renamed to be the Bureau of Alcohol, Tobacco, Firearms, and Software (ATFS).

The new regulations have been taken by most observers as a key indication of the Federal Government's serious concern over the software production scandal gripping the nation. The final verdict of the grand jury investigation into the dangers of unregulated software production was praised as a major victory by software leaders in Redmond last month.

The grand jury investigation centered on the disturbing trend that key portions of the nation's critical infrastructure are being entrusted to a software product for which the secret inner workings (known as `source code') are becoming as prevalent as pornography on the Internet.

The Director of the ATF's 5,000-strong team of agents has pledged his full support to enforce the new regulations, under which all software development must take place only in licensed facilities by trained induhviduals. He was joined at a press conference this morning by the Director of the National Infrastructure Protection Center, who said, "It's about time the ATF took the entire software industry into its jurisdiction." He continued, "We would never consider laying the blueprints for our critical assets out for all to see. I applaud the new regulations for bringing sanity to a long unchecked industry."

The public will have until 1 Jun 2002 to dispose of all unregulated software products they may own. Possession of unlicensed software products can result in penalties up to 20 years in jail and multi-million dollar fines. Currently, only Smallsoft of Redmond, Washington, has achieved the necessary regulatory status to produce software in compliance with the new regulations.

An underground group of activists using the moniker ``the Electronic Frontier Foundation" (EFF) has been strongly critical of the Federal Government's position throughout. Police have indicated the violent clashes are expected between supporters of the EFF and US Presidential nominee Billy Doors, the major proponent of the regulations, as he addresses business leaders in Winnemucca, Nevada, this afternoon.

[I suppose we can understand why they chose the acronym ATFS, given alternatives such as FATS, AFTS, FAST, etc. PGN]<

Category 4D Funny / miscellaneous

2002-04-22 social engineering joke unexpected consequences

RISKS 22 04

At the University of New South Wales, Geoffrey Brent runs a discussion list on which he posted an amusing April Fool's joke to illustrate many of the features of hoaxes. One of the list participants was taken in, however, and vented embarrassingly in front of the whole list. Realizing he'd been fooled, he became nasty and even physically threatening; he eventually had to be thrown off the list. Brent commented in RISKS, "The (April Fool-specific) risks: Forgetting that there will ALWAYS be somebody who doesn't get the joke, no matter how obvious you make it - and that human failure modes are just as bizarre and dangerous as technological ones."

[MK comments: This incident illustrates one of the dangers of any security testing that includes social engineering: embarrassing the victims. I have long held that one should be extremely careful in running social engineering simulations during penetration tests; one way to avoid trouble is to ensure that everyone is prepared for the tests so they can treat the whole thing as a contest.]

Category 4D Funny / miscellaneous

2002-09-30 spam joke funny poem satire spoof parody

NewsScan

#### **OUT, DAMNED SPAM!**

Seeing increasing spam spam in his mail, the NewsScan Poet Laureate, Andrew Rafalski, turned for inspiration to Shakespeare and to Macbeth's famous soliloquy in Act II, Scene I in Shakespeare's play. (Surely you're not surprised that we have our own Poet Laureate!). Here is Andrew Rafalski's Spam Soliloquy: . Is this junk mail which I see before me, And headed my way? Come let me trash you: I keep you not and yet I get you more. Are you not, virtual gunk, sensible To feelings and to right? or are you but A mail for the can, unwanted spam Never to be opened, read or replied? . I get you still, in numbers virtual And unwanted, numbing My mailbox with cache overfilled. You lead me to trash you and revile you, Ignore and defile you. Hotmail and Yahoo I was to use But now both are flooded with Nonsense, gobbledygook and lies. . I see you still, and on your Subject lines, deception, deceit And fabrication. Your marketing Eyes polluting the ether, the net And my mailbox to boot. . Out, damned spam! out, I say! What! will this mailbox ne'er be clea