# INFOSEC YEAR IN REVIEW 2004

as of 2004-12-31

M. E. Kabay, PhD, CISSP mkabay@norwich.edu

Assoc. Prof. Information Assurance Program Director, MSc and BSc in Information Assurance http://www3.norwich.edu/msia http://www2.norwich.edu/mkabay/bsia Division of Business \_Management Norwich University

# 11.1 Data leakage

Category11.1Data leakage2004-01-05Danish Prime Minister accidental information disclosure leakage MS Word PDF

RISKS

DANISH PM'S PRIVATE COMMUNICATIONS DISCLOSED BY MS WORD

Contributor Theodor Norup reports that a press-release Word document from the Danish Prime Minister's Office unintendedly revealed its real source and all its revisions. As a result of this incident, ministry spokesman Michael Kristiansen said the Prime Minister's office would "distribute speeches as PDF files..." Norup believes the risk still is trusting "high echelons of governments" will know a little about information security.

23

12

Category 11.1 Data leakage

## 2004-03-16 Microsoft leaked code Internet vulnerability exploit hacker attacker defense

DHS IAIP Daily; http://www.eweek.com/article2/0,1759,1548988,00.asp

March 14, eWEEK — Leaked code still could bear malicious fruit.

A portion of Windows source code was leaked last month, and researchers are saying that hackers have uncovered several previously unknown vulnerabilities in the code. Immediately following the code's posting on the Internet, members of the security underground began poring over the code, searching for undocumented features and flaws that might give them a new way to break into Windows machines. The real danger isn't the vulnerabilities that this crowd finds and then posts; it's the ones that they keep to themselves for personal use that have researchers worried. Experts said there has been a lot of talk about such finds on hacker bulletin boards and Internet Relay Chat channels of late, indicating that some hackers are busily adding new weapons to their armories. Another concern for Microsoft and its customers is that even though the leaked code is more than 10 years old, it forms the base of the company's current operating system offerings, Windows XP and Windows Server 2003. This means that any vulnerabilities found in Windows NT or Windows 2000 could exist in the newer versions as well.

Category 11.1 Data leakage

## 2004-10-19 spyware Google data leakage shared computers confidentiality

NewsScan; http://www.washingtonpost.com/wp-dyn/articles/A43548-2004Oct18.html

GOOGLE'S PC SEARCH TOOL MIGHT PROVE THE 'PERFECT SPY'

Google Desktop Search, released last Thursday in a "beta" test phase, may prove a boon to disorganized PC users who need assistance in finding data on their computers, but it also has a downside for those who use public or workplace computers. Its indexing function may compromise the privacy of users who share computers for such tasks as processing e-mail, online shopping, medical research, banking or any activity that requires a password. "It's clearly a very powerful tool for locating information on the computer," says one privacy consultant. "On the flip side of things, it's a perfect spy program." The program, which is currently available only for Windows PCs, automatically records any e-mail read through Outlook, Outlook Express or the Internet Explorer browser, and also saves pages viewed through IE and conversations conducted via AOL Instant Messenger. In addition, it finds Word, Excel and PowerPoint files stored on the computer. And unlike the built-in cache of recent Web sites visited that's included in most browser histories, Google's index is permanent, although individuals can delete items individually. Acknowledging potential privacy concerns, a Google executive says managers of shared computers should think twice about installing the tool before advanced features like password protection and multi-user support are available.

# 11.2 Unauthorized disclosure

Category 11.2 Unauthorized disclosure

## 2004-01-10 privacy confidentiality error identity theft

NYT http://www.nytimes.com/2004/01/10/nyregion/10identity.html?th

N.Y.U. notified about 1,800 of its students that their Social Security numbers, phone numbers, and names had been posted on the Internet in a list of students interested in sports. A computer technician in Massachusetts, Brian Ristuccia, republished the information on his Web site and gave it publicity. NYU officials blustered about launching criminal proceedings against Mr Ristuccia, who retorted that he informed the University about the security problem a month before mirroring the data and that it had been available through a search engine.

[MK comments: Although I think it was stupid of Mr Ristuccia to have posted the information himself, it is just as stupid of university officials to focus on blaming him for their own problem.]

# Category 11.2 Unauthorized disclosure 2004-01-12 privacy student personal information Social Security Number SSN New York University NYU

RISKS; http://www.nytimes.com/2004/01/10/nyregion/10identity.html2313STUDENTS' DATA ON WEB, AND NYU ON DEFENSIVE5

Monty Solomon cites an article in \_The New York Times\_ about disclosure of personal information. This article said that New York University had posted the Social Security Numbers, and in some cases, phone numbers, of 1,800 of its students on the Internet. RISKS moderator Peter G. Neumann refers to Dave Farber's comment on this incident: around the time of this incident, NYU had just fired a network security manager who had been working on HIPAA compliance for the university.

Category 11.2	Unauthorized disclosure		
2004-02-02	identity theft fraud threat Department Motor Vehicles		
RISKS		23	16
SECURITY HOLES AT DMVS NATIONWIDE LEAD TO ID THEFT AND SAFETY CONCERNS			

Contributor Monty Solomon says that a report by CDT documents "rampant internal fraud and lax security" at state DMV offices. This report finds that at DMVs, processes "to stop bribery and theft are lacking." Such activities threaten the reliability of drivers' licenses nationwide, says Solomon. The CDT report is titled, "Unlicensed Fraud: How bribery and lax security at state motor vehicle offices nationwide lead to identity theft and illegal driver's licenses"

Category 11.2	Unauthorized disclosure		
2004-02-26	data confidentiality snooping insider crime police database		
RISKS	23	;	23
FBI EMPLOYEE SNO	OPS THROUGH CONFIDENTIAL POLICE DATABASES		
Assistant Attorney Gener	al Christopher A. Wray of the Department of Justice Criminal Division and U.S.	Attorney	Roscoe C.

Assistant Attorney General Christopher A. Wray of the Department of Justice Criminal Division and U.S. Attorney Roscoe C. Howard of the District of Columbia announced that Narissa Smalls, a legal technician in FBI Headquarters, was sentenced to 12 months in prison on charges stemming from her unlawful access of the FBI's Automated Case Support (ACS) computer system.

Category 11.2 Unauthorized disclosure

2004-08-18 PHP-Fusion database backup information disclosure vulnerability

DHS IAIP Daily; http://www.securitytracker.com/alerts/2004/Aug/1010983.html

August 18, SecurityTracker — PHP- Fusion publicly accessible database backups.

A vulnerability in PHP- Fusion 4.0 may allow malicious users to view sensitive data. Path information can be disclosed in error pages by passing invalid input or accessing scripts directly. Additionally, database backup files are placed in a publicly accessible folder with easy to guess names. A remote user can download database backup files, which contain usernames and hashed passwords. This information may allow a remote user to obtain administrative access on the target system. No solution is known at this time.

# Category 11.2 Unauthorized disclosure 2004-09-30 Arizona Motor Vehicle Division sensitive personal information disclosure security flaws

DHS IAIP Daily;

http://www.tucsoncitizen.com/breaking/093004\_mvd\_data\_securi ty.html

September 30, The Associated Press — Arizona MVD has online information security flaws.

The Arizona Motor Vehicle Division's (MVD) information security system has flaws that can expose sensitive personal information, according to a report released Thursday, September 30. The Auditor General's Office said it found no actual security breaches, but auditors detected numerous circumstances that created the potential for misuse of information. Besides data like driver's license numbers, the sensitive information included names, addresses and Social Security numbers. The MVD said it accepted all of the auditors' findings and recommendations and had already started making changes to fix noted shortcomings.

Category 11.2 Unauthorized disclosure

## 2004-09-30 CIA information sharing intelligence community espionage initiative

DHS IAIP Daily;

http://www.fcw.com/fcw/articles/2004/0927/web- info- 09- 30- 04. asp

September 30, Federal Computer Week — Spies work on info sharing.

Officials in the intelligence community have started several initiatives related to information technology tagging, collaboration and acquisition to improve data- sharing among intelligence personnel. One program uses control interfaces to share classified and unclassified data among employees, the Department of Defense, and civilian agencies, according to Alan Wade, chief information officer for the CIA. Another program allows members of the intelligence community to communicate via instant messaging, he said.

Category 11.2 Unauthorized disclosure

2004-10-19 Google Desktop Search sensitive information disclosure share computer risk cybercafés security risk no update issued

DHS IAIP Daily; http://www.informationweek.com/story/showArticle.jhtml?artic leID=50500707

October 19, Associated Press — New Google search tool poses security risk.

People who use public or workplace computers for e- mail, instant messaging and Web searching have a new security risk to worry about: Google's free new tool that indexes a PC's contents for quickly locating data. If it's installed on computers at libraries and Internet cafes, users could unwittingly allow people who follow them on the PCs, for example, to see sensitive information in e- mails they've exchanged. That could mean revealed passwords, conversations with doctors, or viewed Web pages detailing online purchases. Marissa Mayer, director of consumer Web products at Google Inc. said managers of shared computers should think twice about installing the software until Google develops advanced features like password protection and multi- user support.

# Category11.2Unauthorized disclosure2004-12-02government agencies lock down desktop security sensitive data disclosure<br/>prevention

DHS IAIP Daily; http://www.informationweek.com/story/showArticle.jhtml;jsess ionid=TCYMTS5YRH1B0QSNDBGCKHSCJUMEKJVN?articleID=54202021

December 02, InformationWeek — Government agencies lock down desktops.

The Defense and Energy departments are leveraging desktop technologies to shore up security and better protect sensitive U.S. government data. The U.S. Department of Defense is leveraging PC blades to address a longtime concern that electromagnetic waves and stray currents or voltages containing key characteristics of classified data could be intercepted by enemies of the United States and used to reconstruct that classified data and compromise national security. The Energy Department has been shoring up security since it learned that as many as several hundred of its computers were stolen, lost, or improperly inventoried at Los Alamos National Laboratory between 1999 and 2002. For these two departments, security starts at the desktop, where new configurations are being deployed to keep data safely stored away on back- end servers.

# 11.3 Data theft

Category 11.3 Data theft

## 2004-02-13 ATM automated teller machines banks card number PIN theft reader radio

RISKS; http://www.utexas.edu/admin/utpd/atm.html

23

19

INTERESTING DEVICE TO STEAL ATM ACCOUNTS

A team of organized criminals is installing equipment on legitimate bank ATMs in at least 2 regions to steal both the ATM card number and the PIN. The team sits nearby in a car receiving the information transmitted wirelessly over weekends and evenings from equipment they install on the front of the ATM (see photos). If you see an attachment like this, do not use the ATM and report it immediately to the bank using the 800 number or phone on the front of the ATM.

The equipment used to capture your ATM card number and PIN is cleverly disguised to look like normal ATM equipment. A "skimmer" is mounted to the front of the normal ATM card slot that reads the ATM card number and transmits it to the criminals sitting in a nearby car. At the same time, a wireless camera is disguised to look like a leaflet holder and is mounted in a position to view ATM PIN entries.

The thieves copy the cards and use the PIN numbers to withdraw thousands from many accounts in a very short time directly from the bank ATM.

Category 11.3 Data theft

2004-05-06 skimming fraud identity theft

DHS IAIP Daily;

http://www.epaynews.com/index.cgi?survey=&ref=browse&f=view& id=1083842685622215212&block=

May 06, ABC News — Skimming devices implanted in Florida gas pumps.

Credit and debit cardholders in Collier County, FL, have been defrauded out of almost \$500,000 since last October, by criminals who are using card skimmers inside gas pumps to make counterfeit cards for fraudulent purchases. Gas pumps are susceptible to fraud in that they can be opened with a generic key, or a screwdriver, and a skimming device can quickly be attached to the payment hardware inside the pump. By this means, the thieves obtain all the details for counterfeiting cards, namely card numbers and PINs, which can be sold over the Internet for \$20 to \$100 per card. Debit cards, which link directly to consumers' bank accounts, are particularly vulnerable to cloning, as the bank account can be drained while the card is still in the cardholder's possession, and banks may need convincing that the fraud actually happened. South Florida's transient population makes it a target for card thieves, and to this end, some gas stations are asking card- paying customers to provide their zip code as an additional means of verification.

Category 11.3 Data theft

## 2004-05-17 Cisco networking source code leak data theft

DHS IAIP Daily; http://news.com.com/2100-7349-5213724.html

May 17, CNET News.com — Cisco investigates source code leak.

An unspecified amount of the proprietary source code that drives Cisco Systems' networking hardware has appeared on the Internet, the technology giant acknowledged early Monday, May 17. News of the latest source code leak appeared on a Russian security site, SecurityLab.ru, on Saturday, May 15, two days after its administrators received the leaked source code. According to SecurityLab.ru, online vandals had compromised Cisco's corporate network and stolen about 800MB of source code. A person with the alias "Franz" bragged about the intrusion and posted about 2.5MB of code on the Internet relay chat (IRC) system not long after the alleged break- in. "Cisco is aware that a potential compromise of its proprietary information occurred and was reported on a public Web site just prior to the weekend," said Jim Brady, a spokesman for the company. "The Cisco information security team is looking into this matter and investigating what happened." Brady could give no further details on the matter. This is the second time this year that a major technology company's product source code has been made public without authorization. It's uncertain to what degree the leaked code will affect Cisco security.

## Category 11.3Data theft2004-05-18source code theft Cisco Terry Albertstein IOS 12.3 internet main backbone

## NewsScan

## CISCO INVESTIGATING SOURCE CODE THEFT

Cisco has launched an investigation into "a potential compromise" of its intellectual property, a company official says, following reports that some versions of its IOS had been stolen by an individual who broke into the company's corporate network. Terry Alberstein, director of corporate affairs for the Asia-Pacific, said the alleged break-in was not due to any vulnerabilities in Cisco equipment, software or services. He said the company had been made aware of the issue before the weekend, after a report appeared on the Russian security news portal, securitylab.ru. The report said an individual had broken into Cisco's corporate network and stolen the source code for IOS 12.3 and 12.3t. Version 12.3 is used across the Internet's main backbone. The individual who claimed to have accessed Cisco System's corporate network, boasted about it on an underground Internet relay chat channel, claiming that the total amount of data in the archives was around 800 megabytes. Two snippets of code were provided as proof of the claims. (The Age 18 May 2004) rec'd from John Lamp, Deakin U.

## Category 11.3 Data theft

## 2004-09-01 portable handheld digital assistant PDA computer security theft loss encryption confidential data

DHS IAIP Daily; http://www.theregister.co.uk/2004/09/01/pda\_sec/

September 01, The Register — PDA security still dismal.

Worker apathy about PDA security is putting corporate data in jeopardy. The storage of the names and addresses of corporate customers on PDAs is now common - but security practices are struggling to keep up with technology usage. Two thirds of users do not use any kind of encryption to protect confidential data on mobile devices, according to a survey commissioned by Pointsec Mobile Technologies and Infosecurity Europe. The Mobile Vulnerability Survey 2004 found that a third of users do not even use password protection on their devices, leaving the information vulnerable to opportunists, hackers or competitors. The survey findings show that one of the fastest and easiest ways to access corporate data is through unprotected PDAs that are lost or stolen, as they contain business names and addresses, spreadsheets and other corporate documents. One in eight (13 percent) of respondents to the survey have lost their mobile device.

## 12.2 Interception

## Category12.2Interception2004-08-24wiretapping prosecution trial

NYT http://www.nytimes.com/2004/08/24/national/24tape.html?th

Back in 1996, Alice and John Martin illegally intercepted and recorded a cellular phone call involving Newt Gingrich (at that time Speaker of the House). The couple were fined \$500 each for their ctrime. They gave their tape to Rep. Jim McDermott (D-WA), who cheerfully handed it over to the New York Times and the Atlanta Journal-Constitution. In August 2004, a judge finally ruled in a civil suit brought against Rep. McDermott by Rep. John Boehner (R-OH), who had been involved in the call. The judge ruled that Rep. McDermott has violated federal wiretap laws by passing on the tape.

Adam Liptak, writing in the New York Times, wrote an analysis of the legal issues involved:

"The wiretap law makes the knowing disclosure of an illegally intercepted communication both a crime and the basis for a civil lawsuit.

In 2001, however, the Supreme Court ruled that the law was unconstitutional, at least when used to punish disclosure of information about matters of public concern by people who did not themselves participate in obtaining it unlawfully.

`A stranger's illegal conduct does not suffice to remove the First Amendment shield from speech about a matter of public concern,' Justice John Paul Stevens wrote for the majority.

Judge Hogan said that decision did not protect Mr. McDermott because `he knew of the illegality of the Martins' disclosure at the time he voluntarily accepted it.'

That distinction, experts in First Amendment law said, is novel and at odds with the conventional understanding of the Supreme Court's decisions in this area."

Category 12.2 Interception

### 2004-08-30 privacy e-mail law civil liberty Australia warrant SMS law enforcement access

NewsScan

PRIVACY CONCERN OVER AUSTRALIAN E-MAIL LAW

Civil libertarians say that a proposed Australian law could allow authorities easy access to private, stored e-mails without a warrant, giving many new government bodies to access private e-mails, voicemail messages and SMS messages. Under current laws, unopened e-mails can only be accessed if they involve serious crime and only with a telecommunications intercept warrant. If the bill is passed authorities would need only a search warrant, or in some cases no warrant at all, according to online civil liberties group Electronic Frontiers Australia (EFA). (The Australian 30 Aug 2004) Rec'd from J. Lamp

# 13.1 Data diddling

Category 13.1	Data diddling
2004-01-26	Google hacking bomb manipulating search engine query results George W. Bush elections

23

15

RISKS

GOOGLE TARGETED BY PRANKSTERS

Monty Solomon refers us to a \_San Francisco Chronicle\_ article which reports that some Web site operators and bloggers were manipulating search results on Google. These pranksters exploit Google's method of ranking search results to get certain websites ranked better than others for specific queries. This way, the pranksters George W. Bush's biography appear as the top result on the queries "unelectable" and "miserable failure."

Category 13.1 Data diddling

2004-05-11 hacker grade california high school student change grades data

NewsScan

STUDENT HACKER 'MAKES THE GRADE'

A 17-year-old California high school student has been arrested and accused of a felony for allegedly hacking into his school's computer system and changing grades. The arrest came one week after school officials notified police of suspicious grade changes in the academic records of six juniors and one senior. Police Sgt. Steve Shulman says the investigation is continuing because "there may very well be other students involved." Administrators at Corona del Mar High School are examining the records of all 1,500 students to see if any other grades were altered. The charge against the student — "unauthorized alteration of computerized data" — carries a prison sentence of up to three years, but juvenile court officials and prosecutors have not yet decided whether to pursue charges in the case. A spokeswoman for the Newport-Mesa Unified School District says it appears that the records were accessed from a remote location — something that supposedly was not possible — and that the perpetrator was able to circumvent the password authorization feature: "We're upset that we were compromised and we're saddened that these students, who are obviously pretty smart, would use their intelligence for this. We're in a new age. We know that kids will find out what they can do, but we need to be clear that this is illegal — that it's not a game." (Los Angeles Times 11 May 2004)

## **13.2 Data corruption & destruction**

Category 13.2	Data corruption & destruction
2004-11-10	archives digital photography records storage management data corruption loss integrity

## NYT

http://www.nytimes.com/2004/11/10/technology/10 archive.html?th=&pagewanted=print&position=

Katie Hafner reported on a growing problem in November in a New York Times article: digital photographs and other records are much less stable than traditional paper documents. Amateurs lack the awareness and knowledge of the effects of technological obsolescence and are storing their precious data (home movies, photographs of loved ones, personal diaries) on media that are already unreadable because the technology is no longer available: 5" diskettes, old ZIP drives and the like. Worse still, even CD-ROMs are losing data integrity over a period of five years or so if their storage conditions are poor -- and often a single error in a critical area of a file will make the whole photo unreadable. Unlike fuzzy or scratched photos, a scratched CD-ROM may be completely unususable, with the loss of thousands of pictures.

# 14.1Viruses

Category14.1Viruses2004-01-07malware malicious code bogus FBI warning social engineering

The Register

http://www.theregister.co.uk/2004/01/07/bogus\_fbi\_warning\_file\_contains/

BOGUS FBI WARNING FILE CONTAINS MALWARE.

John Leyden of The Register wrote, "Virus writers are attempting to trick music fans into opening malicious code with a message purporting to arise from an FBI investigation into illegal file trading. Recipients of the bogus warning are told they are under investigation. Infectious emails contain an attachment allegedly containing evidence against the 'accused' which actually contains Windows malware, the Melbourne Age reports. The message appears authentic but closer inspection reveals factual errors and spelling mistakes that give the game away. This is the sneakiest piece of social engineering by a virus writer that we can recall."

Link to original article by Sam Varghese in \_The Age\_ of Melbourne: http://www.theage.com.au/articles/2004/01/06/1073268005348.html?oneclick=true

Category 14.1 Viruses

## 2004-01-14 Network Associates Anti-Virus Handhelds ePO Microsoft Pocket PC

NewsBits;

http://www.internetweek.com/breakingNews/showArticle.jhtml%3Bjsessionid=YKFLTHGCLCUBWQSNDBGCKHY?articleID=17300738

Network Associates Adds Anti-Virus Protection For Handhelds

Network Associates on Tuesday added a new anti-virus defense product to its security portfolio, one that targets enterprises with employees carrying Microsoft Pocket PC and Windows Mobile devices. Dubbed McAfee VirusScan PDA Enterprise, the new software installs a small anti-virus client on the mobile gear, but can be managed by the IT staff using Network Associates' McAfee ePolicy Orchestrator (ePO), an verseer's tool that sets and enforces security policies.

Category 14.1 Viruses

## 2004-02-03 virus attack Microsoft escape bounty offer MyDoom worm SCO

NewsScan

MICROSOFT DUCKS, EVADES ASSAULT BY VANDALS

Microsoft has rebuffed an attempted software virus attack aimed at shutting down some of the company's Web sites yesterday — two days after a different version of the same "Mydoom" virus shut down the Web site of The SCO Group in Utah. Microsoft says it will pay \$250,000 to anyone who helps authorities find and prosecute the author of the virus. A similar offer has also been made by The SCO Group. (AP/Washington Post 3 Feb 2004)

Category 14.1 Viruses

## 2004-03-03 virus worm network attack epidemic Netsky

DHS IAIP Daily; http://www.esecurityplanet.com/trends/article.php/3320501

March 02, eSecurity Planet — Virus attacks reach 'epidemic' proportions.

ust as the industry was reeling Monday, March 1, from the weekend release of a new Netsky variant and five new Bagle variants, another two Bagle variants and one more Netsky variant have hit the Internet. Netsky- D, alone, has caused \$58.5 million in damages worldwide, according to mi2g, a London- based security assessment company. And as that variant continues to wreak havoc across the Internet, Netsky- E has been discovered. The latest variant spreads via email and network shares, but so far is not causing as much trouble as its predecessors. "Whoever is behind the Netsky worms is hell bent on causing as much chaos as possible," says Graham Cluley, of Sophos, Inc., an anti- virus and anti- spam company. "They have deliberately released new versions of their virus, tweaked to try and avoid detection by anti- virus software." The Bagle family ushered in Bagle- H and Bagle- I Monday. Bagle- H is an e- mail worm which contains a password- protected Zip file which avoids anti- virus detection. When the attachment is opened, the worm opens up a backdoor on Port 2745 and waits for commands from the virus author. Bagle- I follows the same pattern but has been tweaked to avoid detection by anti- virus software programmed to stop Bagle- H.

## Category 14.1 Viruses

2004-03-25 virus worm writer trial Romania Blaster variant international cybercrime free speech

## DHS IAIP Daily;

March 23, Reuters — Accused virus writer faces trial in Romania.

A decisive test for what is called the "toughest cybercrime law in the world" began Tuesday, March 23, with the opening of a case against a Romanian man charged with spreading a computer virus that affected approximately 1,000 computers. Dan Dumitru Ciobanu is accused of making "Blaster.F," a mild copy of one of last summer's harshest Internet worms. If convicted, the 24- year- old faces between three and 15 years in prison. Romania has enacted tough laws to protect its emerging reputation as a hub of skilled programmers for Western companies and erase any connection with cybercrime syndicates that law enforcement officials say are being run out of Eastern Europe. The Ciobanu case has reignited an international debate on appropriate justice for cybercrimes. With public thirst for cybercrime justice growing, experts wonder what impact a potential stiff sentence on Ciobanu will have on deterring a growing underground of virus writers.

# Category 14.1 Viruses 2004-07-03 Internet Explorer flaw vulnerability hole weakness virus transmission Websites Secunia

NewsScan

WHEN A FEATURE BECOMES A BUG

A report by Secunia, a computer security company, says that an Internet Explorer feature is being used by network vandals to convert Web sites into virus transmitters. (It's not a bug but a feature intended to make browsing more convenient.) Two other flaws in Microsoft products allowed hackers to direct Internet Explorer browsers to automatically run the virus when visiting an infected site. Microsoft says that updated code will be automatically installed on computers set to receive it. The update is also available at http://windowsupdate.microsoft.com. (AP/USA Today 3 Jul 2004)

## Category 14.1 Viruses

## 2004-08-05 portable digital assistant PDA malicious code virus PocketPC Kaspersky

DHS IAIP Daily; http://www.gcn.com/vol1\_no1/daily- updates/26848- 1.html

August 05, Government Computer News — Malicious code targeting PDAs identified.

The first backdoor code for personal digital assistants has emerged, raising concerns that handheld devices soon could be targeted by hackers. The code, called Backdoor.WinCE.Brador.a, was identified by Kaspersky Labs. It is 5,632 bytes and targets PDAs running PocketPC. The Moscow- based antivirus company called Brador a classic Trojan backdoor program, which could expose handheld devices to remote exploitation. Security experts said the threat from Brador is not imminent, but probably is inevitable. The sample seen by Kaspersky was attached to an e- mail from a Russian sender and with Russian text. It creates an executable file in the PDA's autorun folder so that it takes over whenever the device is turned on. It identifies the IP address, contacts the author and opens port 44299 for further commands. The author was offering to sell the client code. PDA users should protect their devices with anti- virus software.

Category 14.1 Viruses

### 2004-08-17 e-mail viruses worms smarter MessageLabs writers spammers collaborations

DHS IAIP Daily;

http://www.reuters.com/newsArticle.jhtml?type=topNews&storyI D=6001506

August 17, Reuters — E- mail viruses getting smarter, report says.

Computer security group MessageLabs, which scans client e- mails for viruses to block, said it picked apart some 5.6 billion e- mails from January to June this year and found 1- in- 12 contained some sort of virus that penetrated firewalls meant to block them. MessageLabs said it believes the biggest e- mail security threat during the first half of 2004 was closer cooperation between virus writers and spammers, writers of unsolicited messages that often advertise products or get people to spend money. The reason the two groups are getting together is profit, MessageLabs has learned through monitoring chat rooms. With the recent proliferation of software blocking spam, the spammers are paying virus writers to create viruses that attach to their e- mails and circumvent the spam blockers.

## Category14.1Viruses2004-08-24Windows 64-bit processor proof-of-concept virus Symantec advisory

DHS IAIP Daily;

http://www.cbronline.com/article\_news.asp?guid=3AF80B03- DE93 - 4EBD- B37F- 41BC1B124C4B

August 24, Computer Business Review Online — First 64- bit Windows virus intercepted.

Anti- virus experts have intercepted the first computer virus targeting 64- bit Windows workstations. According to an advisory issued by Symantec, W64.Shruggle.1318 is a fairly simple "proof- of- concept" virus programmed to attack 64- bit Windows executables on AMD64 systems. Alfred Huger, senior engineer at Symantec Security Response, said it looks like Shruggle has no malicious intent. The virus is not circulating in the wild; Symantec found it on a sample- sharing network used by antivirus firms. "This shows that viruses are being developed for 64- bit processors," Huger said. The worldwide move to 64- bit will not preclude the need for virus detection, he indicated. The virus does not infect 32- bit Portable Executable files and won't run natively on 32- bit Windows platforms. However, it can be run on a 32- bit computer that is using 64- bit simulation software. Original Advisory: http://securityresponse.symantec.com/avcenter/venc/data/w64. shruggle.1318.html

Category 14.1 Viruses

2004-08-26 exam theft virus China black market question papers Microsoft Word Excel

NewsScan

'EXAM THEFT' VIRUS HITS CHINA

A Beijing technology firm, Jiangmin Science Technology, is reporting the discovery of a computer virus specifically designed to steal files labeled "exam" or "test questions." The "exam theft" virus targets Microsoft Word and Excel files, and some observers speculate the virus creators may have been motivated by the thriving trade in black-market exam papers in that region. (The Register 26 Aug 2004)

Category 14.1 Viruses

### 2004-08-30 cybercrime organized virus worm writing spam bot net sales

DHS IAIP Daily; http://www.computerworld.com/securitytopics/security/story/0,10801,95501,00.html?SKC=security-95501

August 30, Computerworld — Organized crime invades cyberspace.

Antivirus researchers have uncovered a startling increase in organized virus- and worm- writing activity that they say is powering an underground economy specializing in identity theft and spam. "The July 2004 outbreak of MyDoom.O was yet another reminder that spammers are now using sophisticated, blended threats that mix spam, viruses and denial- of- service attacks," according to Andrew Lochart, director of product marketing at Postini Inc. According to Mikko Hypponen, antivirus research director at F- Secure Corp., MyDoom.O was the beginning of a concerted, unabashed effort to turn virus and worm infections into cash. Underground bartering and selling is conducted on Websites such as a Russian site that, among other things, sells subscription services to compromised computers. Viruses and worms carrying Trojan horse code are also powering massive identity theft rings. "Whether or not this is traditional organized crime doesn't matter - because they are organized, and what they are doing is criminal," says Hypponen.

 Category
 14.1
 Viruses

 2004-08-31
 Department of Defense DoD viral computer infection Army Space and Missile Defense Command SIPRNET

DHS IAIP Daily;

http://www.fcw.com/fcw/articles/2004/0830/web-siprnet-08-31-04.asp

August 31, Federal Computer Week — DoD reveals viral infection.

Two computers in the Army Space and Missile Defense command connected to the Defense Department's classified Secret Internet Protocol Router Network (SIPRNET) were infected because they did not have any virus protection. William Congo, a spokesperson for the Huntsville, AL- based Space and Missile Defense Command said the two computers were located at a facility in Colorado Springs, CO. The viruses were detected quickly and the two computers were then isolated from the SIPRNET, Congo added. The incident occurred "within the past month" and officials are still investigating the matter to determine how the infection occurred and prevent future occurrences, he said.

# Category 14.1 Viruses 2004-09-20 virus growth volume attacks less successful Symantec Antivirus report zombies infected computers

DHS IAIP Daily;

http://news.com.com/Viruses+keep+on+growing/2100-7349\_3-5374 399.html?tag=nefd.top

September 20, CNET News.com — Viruses keep on growing.

The volume of worms and viruses is increasing, but the rate of successful attacks has dropped, according to a new report from Symantec. The antivirus company's biannual Internet Security Threat Report found that 4,496 new Windows viruses and worms were released between January and June, up more than 4.5 times from same period last year. But overall, Symantec, the daily volume of actual attacks decreased in the first six months of 2004. Alfred Huger, a senior director at Symantec's Security Response team said malicious code writers were increasingly going to spammers to sell them access to the computers that they hack, or break into. Spammers, after paying the hackers, then flood those hacked computers with unsolicited messages, or spam. Symantec also said it expects more viruses and worms in the future to be written to attack systems that run on the Linux operating system and hand- held devices as they become more widely used. The report also noted that the rate at which personal computers are being hijacked by hackers rocketed in the first half of 2004. An average of 30,000 computers per day were turned into enslaved "zombies," compared with just 2000 per day in 2003. Report: http://enterprisesecurity.symantec.com/content.cfm?articleid =1539

Category 14.1 Viruses

## 2004-11-05 computer virus attack New Jersey Motor Vehicle Commission MVC

DHS IAIP Daily; http://www.app.com/app/story/0,21625,1102760,00.html

November 05, Asbury Park Press (NJ) — Computer virus hits state offices.

Drivers and applicants endured sometimes long waits at the newly overhauled New Jersey Motor Vehicle Commission's (MVC) offices on three days last week after a hard- charging computer virus struck its statewide system. Agency spokesperson Gordon Deal said the computer bug zapped, to far lesser degrees, systems in the departments of Treasury, Transportation, and Law & Public Safety. Deal said systems experts do not know where the virus originated or if it had been targeting state computers.

Category 14.1 Viruses

## 2004-11-22 virus trojan SANS MyDoom Trojan.Agent.EC Bofra Virtumonde adware

NewsScan; http://www.internetnews.com/security/article.php/3439011

WHAT EVIL LURKS IN BANNER ADS?

Versions of the MyDoom virus are showing up on banner ads, spreading their misery via compromised ad servers. The SANS Institute Internet Storm Center reports that a "high profile UK Web site" was among those affected and on Sunday, and The Register confirmed that "early on Saturday morning some banner advertising served for The Register by third-party ad serving company Falk AG became infected with the Bofra/IFrame exploit." Falk AG serves ads to many popular sites, including NBC Universal, ATOM Shockwave, The Golf Channel and A&E Networks. In addition to Bofra/MyDoom, two additional viruses are working their way through compromised networks: the first, called Virtumonde Adware, hijacks a server and directs users to different pages and searches than those they had intended. The other, dubbed Trojan. Agent.EC, can take control of a PC through the back door and direct it to upload and execute whatever code the attacker wishes. (Internet News 22 Nov 2004)

## Category 14.1 Viruses 2004-12-07 computer virus infection Jefferson County public schools Kentucky precautions antivirus software

DHS IAIP Daily;

http://www.courier- journal.com/localnews/2004/12/07ky/A1- vir us1207- 5418.html

December 07, The Courier- Journal (KY) — Computer virus infects Jefferson County schools.

Jefferson County public schools in Kentucky are battling a virus that has infected at least 1,000 computers and wreaked havoc on everything from attendance reports to students' ability to finish term papers. Officials blame the same "w32gaobot" virus that hit tens of thousands of school computers statewide late last month, freezing school Websites and barring student access to the Internet. After getting into the state's education computer network, that virus bogged down computers partly by generating overloading traffic on the Internet — and in some cases reading computer passwords and dispersing them and other technical information onto the Internet. Potentially debilitating viruses "show up on a regular basis now," said Cary Petersen, director of technology in Jefferson County Public Schools. One problem controlling viruses in a school system like Jefferson County's, which has about 28,000 computers, is that there are many possible entry points, including spam e- mail attachments, Internet ads or infected floppy disks. Precautions, including anti- viral software and educating workers not to open an e- mail without certain knowledge of its origins, have helped limit the spread, Petersen said.

# 14.2Worms

Category 14.2	Worms
2004-01-02	virus worm network Internet infestation MSN Panda Jitux.A aggressive malicious code

NIPC/DHS; http://www.web-user.co.uk/news/47502.html

December 13, Web User — MSN virus hits the net.

Anti-virus company Panda Software has warned net users to watch out for a new virus, a worm called Jitux.A, which is spread via MSN Messenger. Jitux.A is an aggressive code that contains a link to the web page http://www.home.no// jituxramon.exe. Once open, the file JITUXRAMON.EXE automatically downloads, infecting your computer. The worm file stores itself in the computer's memory and sends new infected messages every five minutes to all contacts in your Messenger's Contact List. Users should update their anti-virus patch as soon as possible.

Category 14.2 Worms

## 2004-01-08 new worm network warning Sophos

NIPC/DHS; http://www.esecurityplanet.com/alerts/article.php/3295121

January 05, esecurityplanet.com — Multi-component worm searches for weak system passwords.

Sophos issued a low-level alert for W32/Randon-AB, a multi-component network worm that attempts to spread by copying components of itself to and executing them on remote ADMINS shares with weak passwords, on Monday, January 5. One component of the worm, B4AK.EXE, then attempts to download and execute a copy of the worm from a remote URL as a file called C:\SVCHOST.EXE. The main file is an SFX EXE which creates a folder called AL within the Windows system folder and drops and executes several files, some of which are legitimate utilities or innocuous files. The worm adds an entry to the registry Run Key to run H00D.EXE on system restart. Instructions for removing worms are at http://www.sophos.com/virusinfo/analyses/w32randonab.htm l

Category 14.2 Worms

## 2004-01-08 MSBlaster worm network patch clean-up removal tool infection Microsoft Windows XP Nachi

NIPC/DHS; http://www.theregister.co.uk/content/56/34751.html

January 07, Register — Microsoft releases Blaster clean-up tool.

Microsoft this week released a tool to clean up systems infected by the infamous Blaster worm and its sundry variants. The software should eradicate the worm from infected Windows XP and Windows 2000 machines. However, users will still have to apply the original patch to prevent re-infection. Normally, such clean-up technology is left to antivirus firms. But this isn't a normal viral epidemic: ISPs say the worm is still generating malicious traffic, months after its first appearance. Microsoft's Windows Blaster Worm Removal Tool will disinfect machines infected with either the Blaster or Nachi worms. Nachi, released shortly after the first appearance of Blaster in August, was designed to patch vulnerable systems. Rather than help out, Nachi has instead become a serious nuisance. Its aggressive scanning behavior blighted the operation of many networks - hence the need to kill the "cure", along with the original Blaster worm. The tool is available at

http://www.microsoft.com/downloads/details.aspx?FamilyID=e70a0d8b-fe98-493f-ad76-bf673a38b4cf&displaylang=en

2004-01-09 worm variant Mimmail network e-mail Sophos

NIPC/DHS; http://esecurityplanet.com/alerts/article.php/3297071

January 08, esecurity Planet — Yet another Mimail variant surfaces.

On the heels of the Mimail.P worm surfacing on Wednesday, January 7, security vendor Sophos issued an alert for the N variant on Thursday, January 8. Like Mimail.P, W32/Mimail-N is a mass-mailing worm that disguises itself as a legitimate form from Paypal credit card information. If a network connection is detected on execution then two forms are displayed asking for credit card and personal information. Once this information is filled in, it is sent to a remote web site. If a network connection is not detected then the start page of Internet Explorer is changed to a web site with a satirical picture. The worm copies itself to ee98af.tmp and winmgr32.exe in the Windows folder and sets the following registry entry so that the latter is run on system startup:HKLM\Software\Microsoft\Windows\CurrentVersion\Run\WinMgr32. This variant also creates a zipped copy of itself as zipzip.tmp in the Windows folder and drops the fake forms as index.hta and index2.hta to the root folder. The worm scans files on the hard disk for email addresses and stores the result in outlook.cfg in the Windows folder. Instructions for removing this variant are at

http://www.sophos.com/virusinfo/analyses/w32mimailn.html

## Category 14.2 Worms

## 2004-01-09 worm variant Mimmail network e-mail Sophos

DHS/IAIP Update; http://www.sophos.com/virusinfo/analyses/w32mimailn.html

January 08, esecurity Planet — Yet another Mimail variant surfaces.

On the heels of the Mimail.P worm surfacing on Wednesday, January 7, security vendor Sophos issued an alert for the N variant on Thursday, January 8. Like Mimail.P, W32/Mimail- N is a mass- mailing worm that disguises itself as a legitimate form from Paypal credit card information. If a network connection is detected on execution then two forms are displayed asking for credit card and personal information. Once this information is filled in, it is sent to a remote web site. If a network connection is not detected then the start page of Internet Explorer is changed to a web site with a satirical picture. The worm copies itself to ee98af.tmp and winmgr32.exe in the Windows folder and sets the following registry entry so that the latter is run on system startup: HKLM\Software\Microsoft\Windows\CurrentVersion\Run\WinMgr32. This variant also creates a zipped copy of itself as zipzip.tmp in the Windows folder and drops the fake forms as index.hta and index2.hta to the root folder. The worm scans files on the hard disk for email addresses and stores the result in outlook.cfg in the Windows folder. Instructions for removing this variant are at

http://www.sophos.com/virusinfo/analyses/w32mimailn.html

Category 14.2 Worms

## 2004-01-20 worm Bagle-A speading Microsoft calculator disguise

NewsScan

NEW COMPUTER WORM: BAGLE-A

A new computer worm called Bagle-A carries an expiration date, giving security experts concern that it might be followed by more robust versions of the now-buggy program. Daniel Zatz, security director for Computer Associates Australia, says, "One of our biggest concern is that if we look back a year ago at the Sobig variants, they all had drop-dead dates, and every time one hit that drop dead date a new variant came out; a new and improved variant of it." Bagle-A arrives in e-mail inboxes as a message containing text suggesting the e-mail may be from a system administrator, as well as an executable attachment. PC users should not open the attachment; if they suspect their computers may be infected with the virus, they should look for a file called bbeagle.exe in their Windows System directory. The file disguises itself under the Microsoft calculator icon. (CNet/New York Times 20 Jan 2004)

## 2004-01-20 worm networkshare infect weak password

NIPC/DHS; http://esecurityplanet.com/alerts/article.php/3299981

January 15, eSecurityPlanet — Worm copies itself to network shares with weak passwords.

W32/Rirc-A is a worm that spreads by copying itself to network shares protected by weak passwords at random IP addresses, according to Sophos, which issued an alert Thursday, January 15. When first run, W32/Rirc-A copies itself to the Windows System folder and appends its pathname to the shell= line in the [Boot] section of \System.ini, so that it is run automatically each time Windows is started. On versions of Windows NT, 2000 and XP the worm also appends its pathname to the following registry entry to run itself on startup:HKLM\Software\Microsoft\Windows NT\CurrentVersion\Winlogon\Shell. Each time the worm runs it tries to connect to random IP addresses on port 139. The worm attempts to logon to the Administrator account of remote computers using a list of 'weak' passwords and if the schedule service is active on the remote computer the worm schedules a new job to run the worm. It also attempts to connect to a remote IRC server and join a specific channel, then sends status information to this channel. More information and instructions for removing the worm can be found at:

http://www.sophos.com/virusinfo/analyses/w32rirca.html

## Category14.2Worms2004-01-21Bagle Internet worm infect spread

NIPC/DHS; http://www.cnn.com/2004/TECH/internet/01/19/bagle.virus.ap/index.html

January 20, Associated Press — 'Bagle' e-mail worm spreading fast.

A new Internet virus was spreading fast throughout Asia, Australia and Europe but computer security experts were divided on the seriousness of the threat from the "Bagle" worm. Experts expected some impact in the U.S. when people returned to work Tuesday, January 20, after a holiday weekend. The "Bagle" or "Beagle" worm arrives in an e-mail with the subject "hi" and the word "test" in the message body. If the accompanying attachment is executed, the worm is unleashed and tries to send itself to all e-mails listed in the user's address book. Sometimes the attachment is designed to look like a Microsoft calculator, said David Perry, spokesman for antivirus software firm Trend Micro Inc. The virus only affects machines running Microsoft Windows operating systems. The worm started spreading on Monday, January 19, and most corporations have already protected themselves against it, Perry said. Carey Nachenberg, chief architect of Symantec Research Labs, said home users, not corporations, were most at risk because companies had protected themselves quickly. "We could see this fizzle out in several days," Nachenberg said. "Or we could also see a lot of people infected" if they don't update their antivirus software.

Category 14.2 Worms

## 2004-01-27 MyDoom virus worm e-mail executable spread

NewsScan

### 'MYDOOM' VIRUS MAKES THE ROUNDS

A new worm is wending its way through corporate networks, masquerading as a normal e-mail message but containing malicious code that propagates itself by mass-mailing more messages at the rate of 200 per minute. It also props open a "backdoor" that leaves the infected computer vulnerable to further misuse. Symantec said the worm — dubbed "Mydoom," "Novarg" or "WORM—MIMAIL.R" — appears to contain a program that logs keystrokes on infected machines, enabling it to collect the username and passwords of unsuspecting users. Network Associates, however, disputed that assertion, saying it had not found any keylogging program. The Mydoom worm spread rapidly yesterday, with about 3,800 infections found within 45 minutes of its initial discovery. "As far as I can tell right now, it's pretty much everywhere on the planet," says Vincent Gullotto, VP of Network Associates' virus response team. The subject lines can vary, but may include phrases like "Mail Delivery System" or "Mail Transaction Failed." The attachments are generally ".exe," ".scr," ".cmd," or ".pif" files and may be compressed as a Zip file. (AP/New York Times 27 Jan 2004)

2004-01-2		worm peer-to-peer Kazaa MyDoom denial-of-service DoS
Category	14.2	Worms

NewsScan

MYDOOM: SAME STUPID SONG, SECOND STUPID VERSE

The e-mail worm Mydoom (also called Novarg or MiMail.r) is back now in a new variant, Mydoom b — which like its predecessor is spread through the Kazaa file-sharing network and is disguised as an e-mail error message. The message bears a variety of subject lines, text and attachment names. Mydoom b launches a denial-of-service attack in which networks are flooded with junk traffic. The Mydoom code includes a message from its creepy author: "I'm just doing my job, nothing personal, sorry." Warning: Don't open an e-mail attachment that you haven't requested or that you have any reason to be suspicious about. (San Jose Mercury News 29 Jan 2004)

Category 14.2	Worms		
2004-02-02	MyDoom SCO worm SoBig denial-of-service DoS network Intern	net	
RISKS	23	3	17
MYDOOM AND SCO			

Contributor Steve Wildstrom writes about the effects of worm MyDoom's denial-of-service attack on SCO's Website in February 2004. He thinks MyDoom had little impact "on the performance of the Internet as a whole." He says that sco.com was not available for the most part starting from Wednesday, January 28. Because of the worm, SCO had to move its Website to www.thescogroup.com. Wilstrom says that judging from the way they handled MyDoom, network administrator were getting better at mitigating worm attacks. In another article about MyDoom, contributor Chris Smith discusses why the worm affected his e-mail account badly. The week of January 26, 2004, Smith received over 30,000 e-mail due to MyDoom. This was about 1000MB worth of messages. He thinks he was so badly hit because he has the popular last name 'Smith', but refuses to believe that his own name is a security risk. Smith thinks MyDoom could have been stopped by the "[I]mplementation of something like Sender Permitted From (SPF)" information in e-mails.

Category 14.2	Worms
2004-02-03	Microsoft MyDoom DoS denial of service worm network attack

## Microsoft MyDoom DoS denial of service worm network attack

DHS IAIP Daily;

http://story.news.yahoo.com/news?tmpl=story&cid=569&ncid=738&e=1&u=/n m/20040203/tc\_nm/tech\_microsoft\_dc

February 03, Reuters — Microsoft site appears to weather MyDoom attack.

Microsoft Corp. appeared to have survived the worst the MyDoom worm could throw at it Tuesday. Experts say the virus, a variant of the myDoom. A virus that knocked out another company's Website Sunday, was programmed to fire continuous volleys of debilitating data at Microsoft's site Tuesday. But there was no visible impact on the software company's Web site, which barely flickered as the MyDoom.B Internet worm's trigger time of 8:09 EST passed. MyDoom.B is a low- grade variant of the original MyDoom.A virus, the fastest- spreading e- mail contagion to ever hit the Internet. MyDoom.A has infected hundreds of thousands, and possibly over one million, PCs, generating a torrent of spam e- mails and crippling corporate e- mail servers, plus slowing traffic for some Internet service providers.

Category 14.2 Worms

#### 2004-02-09 worm virus network attack Microsoft MyDoom variant

NewsScan

'DOOMJUICE' SQUEEZES MICROSOFT

A new worm dubbed "Doomjuice," which some are describing as a variant of the earlier MyDoom worm, is piggybacking on the damage already done by its predecessor by targeting already-infected computers. "It's only looking for machines that are compromised by MyDoom A or B," says Vincent Gullotto, VP of the antivirus emergency response team at Network Associates. Its ultimate target is Microsoft's Web site, which it seeks to overwhelm with distributed denial of service attacks. Microsoft said its Web site is still up and running but the company has offered a \$250,000 bounty for information leading to the capture of MyDoom's author. (Reuters 9 Feb 2004)

## 2004-02-25 worm damage destructive file deletion

http://searchsecurity.techtarget.com/originalContent/0,289142,sid14\_gci952225,00. html?track=NL-102

Yet another Mydoom worm has hit. The new variant targets the Web sites of eternal whipping boy Microsoft and song-swapper foe Recording Industry Association of America.

Mydoom-F works in a way very similar to Mydoom-A — so much so that experts think the creator of Mydoom-F used the source code of the Mydoom-A to create it. The code for Mydoom-A is widely available because Mydoom-B dropped the source code for A on victims' computers.

Mydoom-F does something different than its predecessors. The worm randomly deletes files such as Excel spreadsheets and pictures. This is the first time in recent memory that a worm has been so randomly destructive.

## Category14.2Worms2004-02-26Netsky worm UK email vector F-Secure propagation

DHS IAIP Daily; http://www.vnunet.com/News/1153081

February 26, Vnunet.com — Security vendor mass- mails worm to clients.

Antivirus firm F- Secure has apologized for sending the Netsky.B virus to several thousand of its UK customers and partners via a mailing list. The e- mail apology said: "Because of a human error, you may have received an email infected with the Netsky.B virus that was relayed through our external email list server and was resent to our UK mailing list. The virus did not originate from our network - - it was sent by an unknown party to the list address. If you had up- to- date antivirus installed, the virus has been stopped automatically already and no further steps are necessary on your part." Mikko Hypponen, F- Secure's director of antivirus research, said the mailing list was outside of the firm's normal e- mail scanning. The Netsky.B worm spreads itself in e- mails inside a .zip archive or as an executable attachment. It also copies itself to shared folders of all available drives. This allows the worm to spread through peer- to- peer and local networks.

## Category 14.2 Worms

## 2004-03-04 worm network attach Bagle variant Netsky e-mail

NIPC/DHS

March 03, eWEEK — Tenth variant of Bagle worm hits the Net.

Anti- virus researchers discovered the existence of BagleJ, the tenth variant of the worm to hit the Internet, late Tuesday, March 2. Officials at Network Associates Inc. have rated the worm as a medium risk and said they saw 50 unique samples of BagleJ in a 90- minute period. BagleI also surfaced Tuesday, with Bagle. H appearing Monday. Recent speculation among anti- virus researchers that the creators of the NetSky and Bagle viruses may be engaged in some kind of competition or war has now apparently been proven true. The virus writers have been leaving profane, derogatory messages for one another in the new variants of their respective viruses during the last few days, experts say. Like its predecessors, this version relies heavily on social engineering to entice recipients into opening the e- mail and infected attachment.

# Category 14.2 Worms 2004-03-08 worm network Sober.D SMTP engine masquerading Microsoft update e-mail attachment executable

NewsScan

NEW WORM MASQUERADES AS MS UPDATE

The latest variation on the Sober worm — Sober.D — tries to trick recipients into opening it by disguising itself as a Microsoft Update message. "It arrives in an e-mail that pretends to be a patch to protect against a version of MyDoom," says a senior consultant at antivirus firm Sophos. "The e-mail appears to be a Microsoft patch so people will of course double-click on that attachment." Once a user clicks on the file, the worm scans the PC to see if it's already infected — if not, it installs itself and uses its own SMTP engine to send copies of itself to e-mail addresses found on the victim's PC. Microsoft emphasizes that it does not send patches via e-mail and that users should ignore such messages. (ZDNet 8 Mar 2004)

2004-03-15	Internet worm network password trick foil filters Bagle
Category 14.2	Worms

NewsScan

LATEST E-MAIL WORMS USE PASSWORD TRICK TO FOIL FILTERS

The most recent versions of the pesky Bagle worm — Bagle N and Bagle O — arrive in a compressed and password-locked .zip or .rar file with the password included in the body of the e-mail along with a message urging the recipient to open it right away. This latest technique is designed to foil corporate e-mail filters that may block ordinary zipped attachments but allow password-protected documents to pass through the network's defenses unimpeded. Once the attachment is unlocked, the worm is then forwarded to everyone in the victim's e-mail address book. "The worm's author is sneakily trying to make it more difficult for antivirus products to scan inside the password-protected files," says Graham Cluley, a researcher with U.K cybersecurity firm Sophos. (New Scientist 15 Mar 2004)

Category 14.2 Worms

## 2004-03-16 worm network attack defense failure Bagle variant ZIP

NIPC/DHS

March 15, TechWeb News — New Bagle worm variants sneak past defenses.

Two new versions of the Bagle worm, Bagle.n and Bagle.o, were spotted over the weekend. Unlike earlier editions of Bagle, which tried to circumvent anti- virus software by placing the worm payload into an encrypted .zip archive, the new Bagles may also use a different archive format, .rar, a file type that consumers are unfamiliar with and enterprises may not block at the gateway. Additionally, Bagle.n and Bagle.o include the password to the .rar and .zip files in the message not as text, but as an embedded graphic, a tactic often used to discourage automated e- mail account creation by spammers or by Websites to prevent spam bots from harvesting e- mail addresses. When Bagle first turned to encrypted .zip files to disguise its payloads, anti- virus firms reacted by scanning the message for the in- text password. Shifting to an image of the password may make it tougher for anti- virus programs to unlock the .rar file. The new Bagles randomly attach their code to 32- bit executables on the infected machine's hard drive and then re- infect a supposedly cleaned system once the executable runs.

Category 14.2 Worms

## 2004-03-19 worm network Internet Bagle Outlook flaw exploit

NIPC/DHS

March 18, ZDNet UK — Bagle uses Outlook flaw to speed replication.

Until the appearance of Bagle variants Q, R and S, users had to click on an e- mailed attachment to be infected by the worm. The latest Bagle incarnation has done away with the attachment altogether and spreads when a vulnerable user opens the email using an unpatched version of Microsoft Outlook. If their Outlook preview pane is open, the victim's machine will be compromised automatically. Graham Cluley of Sophos said: "This has the potential to spread very quickly because so many people, particularly home users, have not applied the patches." Mikko Hyppönen of F- Secure said that the latest variant uses a list of about 600 IP addresses, which all seem to be home computers connected to an ADSL service that have been infected by previous versions of Bagle. These "zombie" machines have been updated and are now used to send copies of the new worm to any computer on which the victim uses a vulnerable copy of Outlook to view an infected email message. Outlook uses elements of Internet Explorer to render the HTML for its preview pane, so to avoid the new Bagle worms, users should apply a patch for Internet Explorer that Microsoft released in October 2003.

#### Category 14.2 Worms 2004-03-22 worm network attack security vulnerability flaw exploit firewall BlackIce RealSecure denial-of-service hard disk

## NIPC/DHS

March 20, Washington Post — 'Witty' worm wrecks computers.

A quickly spreading Internet worm exploited a security flaw in a firewall program designed to protect PCs from online threats on Saturday, March 20, computer experts said. The "Witty" worm writes random data onto the hard drives of computers equipped with the Black Ice and Real Secure Internet firewall products, causing the drives to fail and making it impossible to restart the PCs. Unlike many recent worms that arrive as e- mail attachments, it spreads automatically to vulnerable computers without any action on the part of the user. At least 50,000 computers have been infected so far, according to computer security firm iDefense and the SANS Institute. Most infected computers will have to be rebuilt from scratch unless their owners instead decide to buy new ones, said Ken Dunham of iDefense. Joe Stewart of security services company Lurhq said he expects the worm to die out over the next few hours as vulnerable computers quickly become useless hosts. A patch is available the deveoper of the firewalls, Internet Security Systems: http://xforce.iss.net/xforce/alerts/id/167

#### Category 14.2 Worms

#### 2004-03-23 worm network Internet Netsky variant security vulnerability flaw hole exploit

NIPC/DHS

March 22, eWEEK — Netsky.P spreads through ancient security hole.

A new variant of the Netsky worm, Netsky.P, is spreading quickly. This new variant is very much like other Netsky versions with two differences, according to Vincent Gullotto of the McAfee Avert Virus and Vulnerability Emergency Response Team. The initial seating of the worm, referring to the initial group of users to whom the virus author distributed it, appears to have been in Australia. It's not clear whether or how this would facilitate spreading of the worm, but it is unusual. The other unusual characteristic of this worm is that it utilizes a very old vulnerability in Internet Explorer, the Incorrect MIME Header (MS01- 020) bug. This bug, patched almost three years ago, allowed a hostile HTML e- mail to execute arbitrary code if viewed in the preview pane of a mail client. Like other Netsky variants, this one spreads mainly through a built- in SMTP engine to e- mail addresses harvested out of the user's files.

Category 14.2 Worms

#### 2004-03-29 worm network Internet Bagle variant e-mail TCP

NIPC/DHS

March 26, eWEEK — New spawn of Bagle worm unleashed.

Yet another version of the Bagle worm is on the loose and is already causing trouble in parts of Europe. Bagle.U appeared early Friday, March 26, and has begun spreading quickly, even though it contains none of the social engineering tricks that Bagle's author has used to help previous versions succeed. This variant arrives in an e- mail with a blank subject line and no body text. The sending address, as always, is spoofed, and the name of the infected executable attachment is completely random. After execution, the worm mails itself to all of the addresses in the infected machine's address book. Bagle U does include a backdoor component that listens on TCP port 4751 and connects to a Web server in a German domain, www.werde.de, according to Network Associates Inc. Once it establishes a connection with the remote server, the worm generates a unique ID number for each specific infected machine and sends that number and the number of the port on which it is listening to the server. Bagle.U is set to expire on January 1, 2005.

#### Category 14.2 Worms 2004-03-31 worm network Internet NetSky mass-mailing e-mail

NIPC/DHS

March 29, CNET News — NetSky variant a greater threat than thought.

Security company Symantec raised its severity rating of the latest incarnation of the NetSky worm. NetSky.Q was upgraded from a level 2 to level 3 threat on the security firm's five- point rating system. The company said it has received 379 reports of the worm since its discovery Sunday, March 28. NetSky is a mass- mailing worm that uses a bogus sender address and continually changes its subject line and content. An e- mail attachment usually carries an .exe, .pif, .scr or .zip file extension. The worm distributes itself to e- mail addresses in a victim's hard drive and copies itself into shared folders via file- sharing programs. NetSky,Q is expected to release a denial- of- service attack between April 8 and April 11 on several Websites, including those of eDonkey2000, Kazaa, eMule, Cracks.am and Cracks.st, according to Symantec.

## 2004-04-08 worm virus network Netsky e-mail

DHS IAIP Daily; http://www.computerworld.com/securitytopics/security/virus/s tory/0,10801,91978,00.html

April 08, IDG News Service — New Netsky worms change their stripes.

New versions of the Netsky e- mail worm are spreading on the Internet. Netsky.S appeared Monday, April 5, and Netsky.T was detected Tuesday, April 6. They are the 19th and 20th editions of an e- mail virus that first appeared in February. Like its predecessors, the new Netsky variants target machines running versions of Microsoft's Windows operating system. The viruses arrive as files enclosed in e- mail messages that have faked (or "spoofed") sender addresses and vague subjects such as "Re: My details," "Request" and "Thank You!" according to anti- virus company Symantec Corp. Earlier versions of the Netsky variant abstained from opening communications ports that could be used as back doors that remote attackers could use to gain access to compromised systems. However, the latest Netsky variants open a back door on TCP Port 6789 that could be used to receive instructions or malicious code from the worm author.

Category 14.2 Worms

## 2004-04-28 Netsky worm Website Internet denial-of-service Bagle education Windows registry

DHS IAIP Daily; http://www.techweb.com/wire/story/TWB20040428S0006

April 28, TechWeb — Netsky.x lays out Websites.

The Netsky.x worm, which hit the Internet over a week ago and targeted a trio of educational Websites for denial- of- service (DoS) attacks, has laid low two of the three in the first day of its scheduled three- day assault. Version X of the persistent Netsky worm launched a DoS attack on nibis.de, medinfo.ufl.edu, and educa.ch, educational sites from Germany, the United States, and Switzerland, respectively. The DoS attacks, which began Wednesday, April 28, by Netsky.x- infected computers, and is to run through Friday, effectively shut down the German and U.S. sites, according to Ken Godskind of AlertSite, a Web monitoring firm. Other variants released after Netsky.x- - including Netsky.y and Netsky.z- - also targeted the three sites for DoS attacks that could run as long as May 5. The two most recent Netskys, however, dubbed Netsky.aa and Netsky.ab - - which appeared Monday and today, respectively, don't take aim at the educational sites. Instead, Netsky.ab tries to delete the entries of several variations of its rival, Bagle, from the Windows Registry.

Category14.2Worms2004-05-02worm virus malicious code malware Microsoft Windows vulnerability Sasser

DHS IAIP Daily;

http://www.computerworld.com/securitytopics/security/virus/story/0,10801,9285 1,00.html?SKC=news92851

May 02, Computerworld — Worm unleashed that exploits latest Windows security holes, Microsoft warns.

Microsoft Corp. issued an unusual weekend security warning Saturday that a worm has been unleashed on the Internet taking advantage of a security hole announced publicly last month. Microsoft once again urged users to install its most recent critical Windows updates. "Microsoft has verified that the worm exploits the Local Security Authority Subsystem Service (LSASS) issue addressed in Microsoft Security Update MS04- 011 on April 13, 2004," the company said in an announcement posted yesterday and updated 3 a.m. PDT this morning, May 2. In its security update, Microsoft included a tool that checks for system infection by the Sasser worm. Versions of Windows XP and 2000 are vulnerable, although not XP 64- Bit Edition Version 2003, Microsoft said. Both Symantec Corp. and Network Associates Inc.'s McAfee antivirus unit currently rate Sasser as medium risk, while Computer Associates rates it low risk. Trend Micro Inc. says it issued a yellow alert to its customers. For further information: http://www.microsoft.com/security/incident/sasser.asp

# Category 14.2 Worms 2004-05-03 worm virus malicious code malware Microsoft Windows vulnerability Sasser Netsky link

DHS IAIP Daily; http://www.pcworld.com/news/article/0,aid,115964,00.asp

May 03, IDG News Service — Experts probe Sasser, Netsky link.

Analysis of the Sasser and Netsky code reveals many similarities between the two worms, even as a new version of the Netsky e- mail worm appeared on Monday, May 3, that capitalized on fears caused by Sasser Internet worms by posing as an antivirus software patch, experts say. Netsky- AC is the thirtieth version of the mass- mailing e- mail worm to be released since Netsky- A appeared in February. Like earlier versions of Netsky, the AC- variant uses e- mail messages and infected file attachments to spread from computer to computer. A message buried in the worm's code and directed to antivirus vendors claims responsibility for Sasser, which first appeared on Friday, April 30. "Hey av firms, do you know that we have programmed the sasser virus?!? Yeah, thats true," the message reads, in part. The message is attributed to "the Skynet," a virus writing group that also claimed responsibility for other Netsky variants. The worm's author or authors included a sample of the Sasser worm raw "source" code as proof of the legitimacy of the claim, says Graham Cluley, senior technology consultant at Sophos.

## Category 14.2 Worms

## 2004-05-03 worm virus malicious code Finland bank Sasser infection denial of service DoS

DHS IAIP Daily; http://www.heraldsun.news.com.au/common/story\_page/0,5478,94 60659%255E1702,00.html

May 03, Agence France- Presse — Bank closes to ward off virus.

Sampo, Finland's third largest bank, closed its 130 branch offices across the country on Monday, May 3, to prevent the Sasser Internet worm from infecting its systems, officials said. The Sasser bug has so far contaminated millions of computers worldwide, making them shut down and restart in an endless loop. "We decided to close our offices as a precaution, since we knew that our virus protection hadn't been updated," Sampo spokesman Hannu Vuola said. Sampo is Finland's third largest bank with over a million customers nationwide. Its corporate and Internet banking 3 services were not affected by the shutdown, Vuola said.

Category 14.2 Worms

## 2004-05-03 worm virus malicious code malware Microsoft Windows vulnerability Sasser

DHS IAIP Daily;

http://story.news.yahoo.com/news?tmpl=story&cid=1510&ncid=1510&e=2&u=/afp/20040503/tc\_afp/internet\_virus\_taiwan\_040503133241

May 03, Agence France Presse — Taiwan's post office hit by worm.

The new Internet worm, Sasser, that is disrupting computers across the world paralyzed a third of the offices of Taiwan's national post office. Some 1,600 work stations at 430 Chunghwa Post Co. offices, 300 of them in the greater Taipei area, were shut down by the virus Monday, May 3. "We started to receive complaints from offices at around 10:00 am saying their computers kept shutting down and rebooting automatically," a company official told Agence France Presse. "Subsequently manual processes had to be initiated while computer systems were down," the official said. The company said the computer virus had not damaged its computer systems and it expected the virus to be removed by 10:00 pm.

2004-05-03 worm virus malicious code malware Microsoft Windows vulnerability Sasser

DHS IAIP Daily;

http://www.reuters.com/newsArticle.jhtml?type=internetNews&s toryID=5016252&section=news

May 03, Reuters — Sasser worm strikes hundreds of thousands of PCs.

The fast- spreading "Sasser" computer worm has infected hundreds of thousands of PCs globally and the number could soon rise sharply, a top computer security official said on Monday, May 3. "If you take a normal Windows PC and connect to the Internet, you will be infected in 10 minutes without protection," said Mikko Hypponen, Anti- Virus Research Director at Finnish data security firm F- Secure. F- Secure says the worm, which surfaced at the weekend, automatically spreads via the Internet to computers using the Microsoft Windows operating system, especially Windows 2000 and XP. "We have already seen three versions of Sasser during the weekend, and we could see more today," Hypponen said. The current worm does not need to be activated by double- clicking on an attachment, and can strike even if no one is using the PC at the time. When a machine is infected, error messages may appear and the computer may reboot repeatedly.

Category 14.2 Worms

## 2004-05-03 worm virus malicious code malware Microsoft Windows vulnerability Sasser Netsky

DHS IAIP Daily; http://www.esecurityplanet.com/alerts/article.php/3348571

May 03, eSecurityPlanet — Mass- mailing worm copies itself to Windows folder.

Security vendors Monday, May 3, issued an alert for W32/Netsky- AC, a mass mailing worm that copies itself to the Windows folder as comp.cpl and creates a helper component wserver.exe in the same folder. W32/Netsky- AC sets the following registry entry to ensure it is run on user logon: HKLM\Software\Microsoft\Windows\CurrentVersion\Run\ wserver = wserver.exe. Trend Micro also issued an alert for Worm\_Netsky.AC, and reports that this memory- resident worm propagates using its own Simple Mail Transfer Protocol (SMTP) engine. It obtains target email addresses from files with certain extension names, which it searches in drives C to Z (except for CD- ROM drives).

Category 14.2 Worms

### 2004-05-03 Sasser worm train outage Australia RailCorp virus attack

NewsScan

SASSER EYED OVER TRAIN OUTAGE

In Australia, RailCorp has dispatched software engineers to find the source of the outage that left up to 300,000 commuters stranded yesterday, saying the new Sasser worm, which has already spawned two variants, is being evaluated as a possible cause. A RailCorp spokesman confirmed that software engineers were investigating the problem, which prevented drivers from talking to signal boxes. A virus attack was one possibility being investigated. RailCorp was unable to confirm when the investigation would be complete. RailCorp chief executive Vince Graham raised the possibility of a virus attack at a press briefing yesterday: "There is no evidence that hacking is an issue here, the viral infection could have been introduced by one of our own people not taking sufficient care." (The Australian 3 May 2004)

Category 14.2 Worms

2004-05-03 sasser worm F-Secure reboot computers new areas windows Mikko Hypponen threat

NewsScan

SASSER WORM IS LATEST THREAT

A fast spreading worm known as "Sasser" surfaced over the weekend and is making its way around the globe, warn computer security experts at Finland's F-Secure. The worm shares many characteristics with the Blaster worm that infected hundreds of thousands of PCs last year, says F-Secure antivirus research director Mikko Hypponen, who notes that both worms exploit relatively new holes in the Windows operating system and frequently cause computers to repeatedly reboot. However, this time more companies appear to be ready to take preventative action, which may mitigate Sasser's damage potential. "With Sasser it seems that companies are (using software) patches better and more quickly than last year (with Blaster), but for those that are hit, they are hit hard," says Hypponen, who adds that he believes Sasser originated in Russia. The worm does not need to be activated by double-clicking on an attachment and can strike even if no one is using the PC at the time. (Reuters/Washington Post 3 May 2004)

## 2004-05-04 worm IP addresses Windows patch

http://www.nytimes.com/2004/05/04/business/04worm.html?th=&pagewanted= print&position=

The Sasser worm hit the world on April 30, 2004.

The worm spreads through the Internet without user intervention by exploiting a vulnerability in Windows 2000 and Windows XP that had a patch issued by Microsoft on April 12. In addition, "W32.Sasser.Worm can run on (but not infect) Windows 95/98/Me computers. Although these operating systems cannot be infected, they can still be used to infect the vulnerable systems to which they are able to connect." [Symantec Security Response]

Category 14.2 Worms

2004-05-04 worm virus malicious code malware Microsoft Windows vulnerability Sasser

DHS IAIP Daily; http://www.theadvertiser.news.com.au/common/story\_page/0,593 6,9462787%255E421,00.html

May 04, The Australian — Red alert as web worm hits banking.

Staff at Australian banking giant Westpac were forced to revert to pen and paper yesterday as an internet- based computer virus struck Australia and threatened to cause further chaos in the U.S. overnight. Unlike many other viruses, Sasser does not travel by e- mail or attachments and can spread by itself to any unprotected computer linked to the internet. It attacks through a flaw in recent versions of Microsoft's Windows - Windows 2000, Windows Server 2003 and Windows XP- - and causes the computer to shut down, before rebooting it and repeating the process several times. While it slows down computers, it is not believed to cause long- term damage to the hard drive. Internet security company Trend Micro on Monday, May 3, upgraded Sasser to a "red alert" - its highest warning level. Westpac confirmed Monday it was investigating network problems caused by Sasser. Branches had switched to pen and paper manual systems to allow them to keep trading, but the bank's ATM and internet banking networks were not hit, spokesperson Julia Quinn said. The bank expected the problem to be resolved and all systems available at the start of business Tuesday, May 4, she said.

Category 14.2 Worms

### 2004-05-04 computers invaded sasser worm half million PC infect windows

NewsScan

AT LEAST A HALF MILLION COMPUTERS INVADED

The new computer worm called Sasser has already infected hundreds of thousands of computers and caused some networks to crash continually. The worm automatically scans Internet addresses in an infected computer to find another vulnerable PC it can infect. The Microsoft site has a software patch that Windows users should download and install. (New York Times 4 May 2004)

Category 14.2 Worms

2004-05-05 worm virus malicious code malware Microsoft Windows vulnerability Sasser Netsky

DHS IAIP Daily;

http://www.cnn.com/2004/TECH/internet/05/05/sasser.worm.reut /index.html

May 05, Reuters — Hunt on for Sasser worm culprit.

Security experts began the daunting task on Wednesday, May 5, of trying to track down the authors of "Sasser," a tenacious computer worm expected to infect millions of machines before it runs its course. Home users, corporations, and government agencies throughout Europe, North America and Asia have been hit. Once infected, the vulnerable PC reboots without warning as the compact program hunts for more machines to infiltrate. Microsoft (MSFT.O) said on Wednesday it had not made a decision to issue a reward for information leading to the arrest of the Sasser author. Over the past six months, the software giant has offered three separate \$250,000 rewards for previous outbreaks - so far, with no results. Microsoft said it is working with U.S. law enforcement authorities, including the Federal Bureau of Investigation, to flush out the culprits.

2004-05-05 worm virus malicious code malware Microsoft Windows vulnerability Sasser Netsky

DHS IAIP Daily; http://www.gcn.com/vol1\_no1/daily-updates/25838-1.html

May 05, Government Computer News — Sasser worms slowing the Internet.

The Sasser family of worms appears to be slowing down Internet traffic and making some destinations unavailable, according to observations by Keynote Systems Inc., a Web performance management company. "Reachability has crept down and we saw a spike in that at 8 p.m. Eastern Time, Tuesday, May 4, accompanied by an upward spike in packet loss," said Kirsten Husak, a consulting manager in the San Mateo, CA, company's professional services division. "It is definitely more than normal Internet variability." But the worms' impact is not as severe as some past outbreaks, such as last year's Slammer. "This doesn't seem to be affecting Web sites nearly as much." Sasser, which exploits a Microsoft vulnerability announced with the release of a patch in mid- April, first appeared May 1, and began spreading rapidly. It is believed to be the first self- executing worm and does not require any recipient action to propagate. It instructs vulnerable systems to download and execute the viral code. By May 3, four variants of the worm were in the wild, and thousands of computers had been infected. The number of infected computers has since been estimated at more than one million.

## Category 14.2 Worms

## 2004-05-05 sasser creator authorities U.K. teaming up security experts Netsky

NewsScan

AUTHORITIES TEAM UP ON HUNT FOR SASSER CREATOR

Security experts in the U.K. are teaming up with U.S. law enforcement officials to track down the author or authors of the Sasser worm and are investigating the theory that the creator is part of a Russian group calling itself the "Skynet antivirus group," which also was responsible for the Netsky e-mail virus outbreak. A message found in the code of a recent Netsky variant claimed responsibility for Sasser, but the reasoning behind this latest Internet assault is still murky. "With Sasser, the author seems to be showing off his coding capabilities, but otherwise I have no idea what the motive is," says Raimund Genes, European president of antivirus group Trend Micro. And while Microsoft has yet to decide whether to offer a reward for information leading to culprit, most experts agree if the originators are linked to criminal groups, a bounty offer will have little effect. "If the person doesn't disclose his identity, we will never know the author of this worm or the author of those worms that have caused global epidemics in the past," says Eugene Kaspersky, co-founder of Moscow's Kaspersky Labs. Over the past six months, Microsoft has offered three separate \$250,000 rewards for previous outbreaks, but with no results. (Reuters/Washington Post 5 May 2004)

Category 14.2 Worms

2004-05-06 worm virus malicious code malware Microsoft Windows vulnerability Sasser

DHS IAIP Daily; http://www.computerworld.com/securitytopics/security/virus/s tory/0,10801,92936,00.html

May 06, Reuters — Security experts warn of nastier Sasser worm.

Computer security experts warned Wednesday, May 5, that the Sasser worm could merge with earlier viruslike programs to wreak more havoc on the Internet. Since appearing over the weekend, the fast- moving Sasser computer worm has hit PC users around the world who run the ubiquitous Microsoft Windows 2000, NT and XP operating systems. It is expected to slow down as computer users download antivirus patches. But Sasser could mutate by combining with the 2- month- old Netsky worm and become a launching pad for further Web attacks, putting it on par with Blaster, the destructive worm that appeared last year and used infected computers to attack Microsoft Corp.'s Web site. "My expectation is that Netsky and Sasser variants will merge and become what we call one 'abundant threat' that attacks through e- mail and software vulnerabilities," said Jimmy Kuo, a research fellow at Network Associates Inc.'s McAfee antivirus unit.

## 2004-05-10 worm virus malicious code malware Microsoft Windows vulnerability Sasser

DHS IAIP Daily;

http://www.cnn.com/2004/TECH/internet/05/10/computer.worm.ap/index.html

May 10, Associated Press — New Sasser worm may be circulating.

An 18- year- old German who confessed to creating the "Sasser" computer worm apparently released a new version of the program shortly before he was arrested last week, investigators said Monday, May 10. German investigators said Microsoft had reported some computer users were having problems with "Sasser e," a variation of the original worm. Frank Federau, a spokesperson for the state criminal office in Hanover, said the worm was "a slightly modified form" of the program that raced around the world over the past week, exploiting a flaw in Microsoft's Windows operating system. The suspect likely programmed it "immediately before his discovery," he said. Four versions of Sasser were already known. Police have said the German teenager was responsible for all of them in addition to the "Netsky" virus. The teenager has told officials that his original intention was to create a virus, "Netsky A," that would combat the "Mydoom" and "Bagle" viruses, removing them from infected computers. During that effort, he developed the Netsky virus further - - and after modifying it created Sasser.

Category 14.2 Worms

### 2004-05-11 worm virus malicious code malware Microsoft Windows vulnerability lsass

DHS IAIP Daily; http://www.esecurityplanet.com/alerts/article.php/3352151

May 11, eSecurity Planet — New worm mimics Sasser, exploits LSASS vulnerability.

The arrest of the alleged creator of the Sasser worms has not been accompanied by a lull in the momentum of computer viruses. Panda Labs has detected the appearance of a new worm, Cycle.A W32/Cycle.A.worm, which, like Sasser and its variants, exploits the LSASS vulnerability affecting some Windows versions in order to infect computers through the Internet. The scenario has changed, however, as indicated by the text found inside the virus code. In this text, the virus creator - - alias Cyclone - - claims to be Iranian and refers to the social and political situation in his country. Cycle.A tries to enter computers through communications port TCP45 in order to check if the system is vulnerable. If it is, the worm causes the affected computer to download a copy of itself called CYCLONE.EXE. However, this will only take place if the application TFTP.EXE is installed on the system. Additionally, and regardless of whether the worm has managed to copy itself to the targeted computer, the attempt by the virus to enter the system causes a failure in the application LSASS.EXE which makes the computer restart every 60 seconds. Users should install the Microsoft patch available from: http://www.microsoft.com/technet/security/bulletin/MS04- 011. mspx.

## Category 14.2 Worms 2004-05-12 worm virus malicious code malware Microsoft Windows vulnerability Sasser German police raid

DHS IAIP Daily;

http://story.news.yahoo.com/news?tmpl=story&ncid=1212&e=6&u= /afp/20040512/tc\_afp/internet\_virus\_germany&sid=96001018

May 12, Agence France- Presse — German police raid homes in Sasser computer worm probe.

German police have raided the homes of five people who had been in contact with a teenager arrested last week on suspicion of creating the Sasser computer worm, police spokesman Detlef Ehrike said. Investigators "suspect that other people took part in spreading the worm. The Verden prosecutors office ordered raids in the Rotenburg an der Wuemme region," Ehrike said. The 18- year- old German, whom police have not identified by name, was arrested Friday, May 7, after a raid on his parents' house turned up incriminating evidence. Acting on a tip off from computer giant Microsoft, investigators seized several items from the house, including the teen's personal computer. He faces up to five years in prison for "computer sabotage" if found guilty of creating and spreading the computer worm. The Sasser worm struck on May 1, and in less than a week affected thousands of companies and as many as 18 million computers worldwide, forcing some businesses to shut temporarily in order to debug their systems. The teenager is also suspected of creating Netsky.ac; a worm that also spread across the Internet early last week. "Two suspects have admitted receiving from the author of Sasser the source code for the Netsky worm," Ehrike said, adding that one of them had admitted to "taking part in spreading the Netsky worm."

## Category 14.2 Worms 2004-05-17 worm virus malicious code malware Microsoft Windows vulnerability Sasser Dabber "good" worm

DHS IAIP Daily; http://www.computerworld.com/securitytopics/security/virus/s tory/0,10801,93154,00.html

May 17, IDG News Service — New worm targets Sasser code flaw.

A new Internet worm called Dabber is believed to be the first worm that spreads by specifically targeting a flaw in another worm's code, according to LURHQ Corp., a managed security services company. Using code written to exploit the FTP flaw, the recently released worm scans the Internet for Port 5554 to identify computers running Microsoft Corp.'s Windows operating system that are infected with Sasser, LURHQ said. When it finds vulnerable hosts, it connects to the victim and uses a built- in FTP server to transfer the worm file, named package.exe, to the system. When it runs, the Dabber worm installs itself on Windows and then shuts down the Sasser worm and other worm processes, preventing them from running again. Dabber also opens TCP Port 9898 as a back door, which can be used by a remote attacker to download other code or communicate with the infected host, LURHQ said. The original advisory and insturctions for shutting down and removing Dabber are available here: http://www.lurhq.com/dabber.html

Category 14.2 Worms

## 2004-05-17 worm vulnerability IRC chat worm krisworm

DHS IAIP Daily; http://www.esecurityplanet.com/alerts/article.php/3354731

May 17, eSecurity Planet — Worm acts with MIRC client to allow remote access.

IRC/Krisworm- C is a worm used in conjunction with a MIRC client to allow remote access to the host computer, according to Sophos, which issued an alert Monday, May 17. It has the same characteristics as W32/Krisworm- A, a worm that spreads by targeting computers with weak administrator and user passwords. The worm installs several files in the fonts subfolder of the Windows fonts folder, and also attempts to propagate via peer- to- peer (P2P) file- sharing networks. It can also propagate via IRC and via newsgroups. It terminates running antivirus and firewall software. It runs on Windows 95, 98, ME, NT, 2000, and XP. More information at: http://www.sophos.com/virusinfo/analyses/irckriswormc.html

## Category14.2Worms2004-06-03Harry Potter game masquerading worm virus Internet Sophos

NewsScan

POTTER-MANIA FUELS NETSKY.P WORM

The popularity of the latest Harry Potter film, which debuted in Britain Monday, is spurring the resurgence of the Netsky.P worm, which is now disguising itself as a Potter game, warn antivirus experts. Computer security firm Sophos says it has spotted thousands of copies in the last few days. "Echoing a technique used in 2000 by the Pikachu worm, Netsky.P targets young computer users by sometimes posing as content connected with the Harry Potter books and movie franchise," says Sophos senior tech consultant Graham Cluley. "Parents need to educate their children against the threats of viruses, to ensure the popularity of Potter doesn't cast a nasty spell on their computer systems." (BBC News 3 Jun 2004)

Category 14.2 Worms

## 2004-08-03 MyDoom variant Yahoo People Search Internet proliferation SANS report

DHS IAIP Daily; http://www.eweek.com/article2/0,1759,1630964,00.asp

August 03, eWEEK — New MyDoom variant uses Yahoo People Search.

Another new version of MyDoom is worming its way through the Internet. MyDoom.P arrives via e- mail, with a spoofed sending address and a subject line designed to make it look like the message is related to one that the recipient sent. The body of the e- mail contains any of a number of sentences, some of which refer to the included Zip file. Once opened, the executable file copies itself to the Windows system directory as "winlibs.exe." The executable contains a list of dozens of common first and surnames that it puts through Yahoo's People Search in an attempt to find more e- mail addresses to mail itself to, according to the Internet Storm Center at The SANS Institute. Researchers on Monday discovered a new version of the Gaobot worm, which spreads through the back doors installed by MyDoom variants, among other avenues of infection. Gaobot.BAJ connects to an IRC server on port 6667 and waits for instructions from the attacker. It then begins scanning the local network for machines sharing resources with the infected PC and tries to copy itself to those machines. Afterward, it begins scanning for PCs infected with any of the MyDoom worms and attempts to install itself through the back door these worms place on infected computers.

2004-08-09 Bagle worm variant ZIP file Trojan creation viral download

DHS IAIP Daily; http://www.eweek.com/article2/0,1759,1633739,00.asp

August 09, eWEEK — Bagle variant exacts a 'price' with infected zip files.

Another variant of the Bagle worm began making its way across the Internet on Monday, August 9. Bagle.AQ arrives via an e- mail message with a spoofed sending address and no subject line. The only text in the message body is typically one or two words, either "price" or "new price." The name of the infected Zip file that accompanies the message is some variation on that theme as well. The files often are named Price.zip or New\_price.zip, and may have a number appended to the end of the file name. Some users reported getting as many as 100 infected messages in an hour. If a user opens the Zip file with an application such as Windows Internet 13 Explorer that is not a standalone Zip file handler, the user will see an HTML file that contains exploit code. The file will then execute an included .exe file, which is a Trojan, according to McAfee Inc.'s analysis. The Trojan then connects to a number of remote sites to download the actual viral code. Because it can inject itself into the Explorer process space, the worm's outgoing traffic will appear legitimate to most firewalls.

Category 14.2 Worms

2004-08-12 MS Blaster virus worm network creator writer teenager guilty plead Minnesota

NewsScan

TEEN PLEADS GUILTY OVER BLASTER

A Minnesota teenager has pleaded guilty to creating and spreading a variant of the MS Blaster virus that wreaked havoc on thousands of computers around the world last year. He now faces between 18 months and three years in jail and could be ordered to pay millions of dollars in restitution for the damage. (The Australian 12 Aug 2004) Rec'd from J. Lamp

# Category 14.2 Worms 2004-08-16 MyDoom worm variant e-mail spread executable file photo Trojan Horse Internet download

DHS IAIP Daily; http://www.theregister.co.uk/2004/08/16/mydoom\_spam/

August 16, The Register — Infected PCs spew MyDoom variant.

The MyDoom worm saga continued Monday, August 16, with the release of yet another variant of the e- mail worm. The latest variant - MyDoom- S (AKA MyDoom- Q or MyDoom- R) - poses as a funny photographs in order to dupe users into opening an infectious attachment called photos\_arc.exe. MyDoom- S runs when a Windows user clicks on this malicious attachment. Thereafter the worm mass- mails itself to email addresses harvested from the infected machine with the subject line "photos" and message body "LOL!;))))". Like other variants of MyDoom, MyDoom- S tries to download a backdoor Trojan (in this case Surila- G) from one of a number of Websites onto infected PCs. The Trojan allows infected machines to be controlled remotely by attackers in order to send spam, for example.

## Category 14.2 Worms

## 2004-08-17 unsecure unprotected personal computer PC worm infection 20 twenty minutes Internet SANS

DHS IAIP Daily; http://www.gcn.com/vol1\_no1/daily- updates/26967- 1.html

August 17, Government Computer News — Unprotected PCs can expect infection in minutes.

The average survival time for an unprotected networked computer dropped from 40 minutes to 20 minutes over the last year, according to the SANS Institute of Bethesda, MD. That means that an unprotected PC can expect to become infected by a worm within 20 minutes of being connected to an unprotected network. "The actual time it will take for a specific computer to be compromised will vary widely depending on any filters applied by the Internet Service Provider and the configuration of the operating system," the institute said. But the trend reflects the narrowing window of opportunity for users to adequately protect networked computers from known vulnerabilities. Survival time is figured from daily reports submitted to SANS' Internet Storm Center by volunteers in 70 countries. ISC receives more than one billion reports of probes each month from organizations that manage more than 500,000 Internet addresses. The 20- minute figure represents the overall average time between probes on a targeted PC.

## Category14.2Worms2004-08-19Internet worm spread instant messenger IM ICQ Outlook PivX

DHS IAIP Daily; http://www.pcworld.com/news/article/0.aid.117481.00.asp

August 19, IDG News Service — New worm travels by IM.

Security researchers at PivX Solutions have intercepted new malicious code closely resembling that from widespread attacks in June credited to a worm named "Scob" or "Download.ject." The Scob in June attacks were attributed to a Russian hacking group known as the "HangUP team." The attacks begin with instant messages sent to people using America Online's AOL Instant Messenger or ICQ instant messaging program inviting recipients to click on a link to a Web page. The messages could appear to be sent from strangers or from regular IM correspondents, Larholm says. Victims are routed to Websites hosted on servers in Uruguay, Russia, and the United States. The code on the sites takes advantage of vulnerabilities in Microsoft Internet Explorer and Outlook. Though Microsoft patched those vulnerabilities in MS03- 025 and MS03- 040, released in 2003, the attackers are attempting to exploit unpatched systems. In addition to opening a "back door" on the victim's computer, the new attacks change the victim's Web browser home page or Outlook e- mail search page to Websites featuring adult content, Thor Larholm of PivX says. "And as with the Scob attacks, this is all about money- - in this case, driving ad revenue for specific people."

# Category 14.2 Worms 2004-12-09 2004 worm outbreak Netsky-P worst Sophos Security report German teenager Sven Jaschan

DHS IAIP Daily; http://www.govtech.net/?pg=news/news&id=92407

December 09, Government Technology — Netsky- P tops list of year's worst virus outbreaks.

Sophos, a leading security company, released a report revealing the hardest hitting viruses of 2004. In a year which saw a 51.8 percent increase in the number of new viruses, the Netsky- P worm has accounted for almost a quarter of all virus incidents reported, making it the hardest hitting virus of 2004. Sophos researchers have identified 10,724 new viruses so far in 2004 bringing the total viruses in existence to 97,535. German teenager Sven Jaschan, who wrote both the Netsky and Sasser worms, is responsible for more than 55 percent of all virus reports in 2004. Jaschan was apprehended and confessed to his involvement in May 2004, but his worms continue to spread. In November 2004, eight months since its original discovery in March, Jaschan's Netsky- P worm was still the world's most widely reported virus. Also, the United States continues to lead the world in spam, accounting for more than two of every five spam emails. Over 40 percent of spam comes from PCs that have been hijacked by viruses. Despite an increase in law enforcement, the volume of threats, such as viruses and spam, continues to rise.

Category 14.2 Worms

## 2004-12-28 Cabir smart phone worm source code released Internet Kaspersky F-Secure

DHS IAIP Daily; http://www.eweek.com/article2/0,1759,1745949,00.asp

December 28, eWeek — Source code for Cabir cell phone worm released.

Anti- virus vendors are bracing for a deluge of new and potentially dangerous mutants of the Cabir worm on smart phones running the Symbian Series 60 software. That's because the source code used to create the original Cabir worm has been posted on the Internet by a member of an international virus- writing group. According to an advisory from Kaspersky Lab senior virus analyst Aleks Gostev, the Cabir source code was previously accessible only to a limited number of people, including members of 29A, an international virus- writing group. According to information released by security research firm F- Secure, at least seven Cabir variants and one new strain of the Skulls Trojan have been detected this month alone. The first Cabir worm was discovered in June. F- Secure virus tracker Jarno Niemela said all the new variants appear to be recompiled versions based on original Cabir source code, confirming fears that the source code has been made public. Even though the worm has not been directly destructive or malicious, it is capable of blocking normal Bluetooth connectivity and completely draining the battery power from the infected phone.

## 14.3 Virus/worms

Category 14.3 Virus/worms

## 2004-02-17 virus worm Bagle network Internet spread momentum

DHS IAIP Daily;

http://www.eweek.com/article2/0,4149,1528349,00.asp?kc=EWRSS03119TX1K00 00594

February 17, eWEEK — New Bagle virus gaining momentum.

A new version of the Bagle virus is making the rounds of the Internet. Known as Bagle.B, the virus is a mass- mailer like the original Bagle and also includes a component that notifies the author each time a new machine is infected. The new variant arrives in an e- mail with a spoofed sending address and a subject line that contains the term "ID" followed by a string of random characters. The text of the message simply says: "Yours ID" followed by another bunch of random characters. The attachment is an executable file with a random file. Once the user executes the file, the virus mails itself to all of the names found on the user's hard drive, with the exception of addresses in the Hotmail, MSN, Microsoft and AVP domains. Bagle.B also opens port 8866 and begins listening for remote connections, according to Network Associates Inc. The virus also sends an HTTP notification, presumably to the author, notifying him that the machine is infected.

Category 14.3 Virus/worms

### 2004-02-18 Netsky worm virus network Internet variant warning Netsky.B

DHS IAIP Daily;

2004-02-18

http://www.computerworld.com/securitytopics/security/virus/story/0,10801,9026 4,00.html

Experts warn of new NetSky worm variant.

Anti- virus software companies are warning that a new version of the NetSky e- mail worm is circulating on the Internet. NetSky.B, also known as Moodown.B, first appeared Wednesday, February 18, and is spreading through infected e- mail messages and shared network folders. Once installed, NetSky tries to disable antivirus software, steal e- mail addresses and copy itself to shared network folders, anti- virus companies said. The new worm is a modified version of NetSky.A, which appeared on Monday. Like its predecessor, NetSky.B arrives in e- mail messages that have randomly generated subject lines such as "something for you," "hello" or "fake." The worm file is contained in a zipped attachment that also has a randomly generated name and file type such as "document" "stuff" or "party." Most copies of the worm appear to be coming from the Netherlands and elsewhere in Europe. Users are advised to update their anti- virus software as soon as possible.

Category 14.3 Virus/worms

## Netsky worm virus network Internet variant warning Netsky.B

DHS IAIP Daily; http://www.computerworld.com/securitytopics/security/virus/story/0,10801,9026 4,00.html

February 18, Federal Computer Week — Experts warn of new NetSky worm variant.

Anti- virus software companies are warning that a new version of the NetSky e- mail worm is circulating on the Internet. NetSky.B, also known as Moodown.B, first appeared Wednesday, February 18, and is spreading through infected e- mail messages and shared network folders. Once installed, NetSky tries to disable antivirus software, steal e- mail addresses and copy itself to shared network folders, anti- virus companies said. The new worm is a modified version of NetSky.A, which appeared on Monday. Like its predecessor, NetSky.B arrives in e- mail messages that have randomly generated subject lines such as "something for you," "hello" or "fake." The worm file is contained in a zipped attachment that also has a randomly generated name and file type such as "document" "stuff" or "party." Most copies of the worm appear to be coming from the Netherlands and elsewhere in Europe. Users are advised to update their anti- virus software as soon as possible.

# Category 14.3 Virus/worms 2004-02-26 Netsky new virus worm variation pornography hacking MP3 deception social engineering

DHS IAIP Daily; http://www.web- user.co.uk/news/48008.html

February 26, Webuser (UK) — New version of Netsky worm appears.

A new version of the Netsky worm has been detected that snares internet users by disguising itself as pornography or documents about hacking or MP3s. Once one of these files is opened, the Netsky.C infects the user's computer and sends a copy of itself to e- mail addresses on the infected computer. It can also spread via file sharing networks such as Kazaa and the ICQ chat system. According to security experts, Netsky.C is similar to its predecessor Netsky.B as both spread by e- mail and file sharing networks. When it spreads via e- mail it selects random names for the subject line and file name. When first run, Netsky.C copies itself to the Windows folder as winlogon.exe and creates the following registry entry: HKLM\Software\Microsoft\Windows\CurrentVersion\Run\ICQNet= \winlogon.exe - stealth', so that winlogon.exe is run automatically each time Windows is started. Netsky.C also copies itself to folders on drives C to Z whose name contains the sequence of letters 'Shar', this includes shared folders and explains how it spreads through P2P file sharing where users download from each others' shared folders.

# Category 14.3 Virus/worms 2004-05-12 worm virus malicious code malware Microsoft Windows media player vulnerability Wallon

DHS IAIP Daily; http://news.zdnet.co.uk/0,39020330,39154533,00.htm

May 12, ZDNet (UK) — Wallon virus wrecks Windows Media Player.

A new mass- mailing virus called Wallon was discovered in Europe on Tuesday, May 11. Maikel Albrecht of security company F- Secure said that because of recent virus outbreaks, users are less willing to open e- mail attachments, which is why Wallon's author is counting on users clicking on an e- mail link instead. "The link in the email points to the actual virus, so if you click the link you download the virus," said Albrecht. However, once the PC is infected, Wallon remains dormant until the user tries to run a media file such as an MP3 or a video. If by default the system uses Windows Media Player, the virus is activated and attempts to send HTML emails, each with a link to the virus file, to any email addresses in the computer's address book. Wallon requires intervention by the user before it can replicate, so Albrecht expects it will not spread very quickly. But unlike common viruses, Wallon is destructive because it replaces the wmplayer.exe file, which means that users infected by the worm will need to reinstall Media Player. Stuart Okin of Microsoft UK said anyone worried about Wallon should install Microsoft's MS04- 13 patch, which was released in mid- April and solves the problem.

Category 14.3 Virus/worms

### 2004-06-18 Sasser worm creator writer interview Germany

NewsScan

SASSER CREATOR INTERVIEWED

In an interview with the German magazine Stern, Sven Jaschan, the author of the Sasser worm that hit Windows users at the beginning of last month, says it was one of his friends who tipped off Microsoft in an attempt to claim a reward. (The friend is now also under suspicion for his involvement with writing and distributing the virus, and Microsoft has indicated there will be no reward.) Jaschan says he inserted into Sasser a piece of code he found on the Internet that "malfunctioned" and caused PCs to reboot. He claims this was not his intention, and that he was

"thoughtless" in not considering the consequences or the damage his worm would cause. (The Age 18 Jun 2004) Rec'd from John Lamp, Deakin U.

# 14.4 Trojans

Category 14.4 Trojans

## 2004-01-08 Trojan horse malicious agent back door HTML

NIPC/DHS; http://www.esecurityplanet.com/alerts/article.php/3295891

January 06, esecurityplanet.com — Trojan sends spammed message with woman's picture.

BackDoor-AWQ.b is a remote access Trojan written in Borland Delphi, according to McAfee, which issued an alert Tuesday, January 6. An email message constructed to download and execute the Trojan is known to have been spammed to users. The spammed message is constructed in HTML format. It is likely to have a random subject line, and its body is likely to bear a head portrait of a lady (loaded from a remote server upon viewing the message). The body contains HTML tags to load a second file from a remote server. This file is MIME, and contains the remote access Trojan (base64 encoded). Upon execution, the Trojan installs itself into the %SysDir% directory as GRAYPIGEON.EXE. A DLL file is extracted and also copied to this directory (where %Sysdir% is the Windows System directory, for example C:\WINNT\SYSTEM32) The following Registry key is added to hook system startup:

HKEY\_CURRENT\_USER\Software\Microsoft\Windows\CurrentVersion \RunOnce "ScanRegedit" = "%SysDir%\GRAYPIGEON.EXE" The DLL file (which contains the backdoor functionality) is injected into the EXPLORER.EXE process on the victim machine. More information, including removal instructions, can be found at: http://us.mcafee.com/virusInfo/default.asp?id=description &virus\_k=100938

# Category 14.4 Trojans 2004-01-09 malware Microsoft trojan horse Windows Update social engineering swen Xombe Dloader-L

NewsBits; http://www.gcn.com/vol1\_no1/daily-updates/24599-1.html http://computerworld.com/securitytopics/security/story/0,10801,88940,0

New malware masquerades as Microsoft update

A Trojan horse program that appears to be a Microsoft Corp. security update can download malicious code from a remote Web site and install a back door on the compromised computer, leaving it vulnerable to remote control. Idefense Inc., a Reston, Va., computer security company, said the malicious code is the latest example of so-called social engineering to fool Windows users. It is similar to the W32Swen worm, which last year passed itself off as a Microsoft patch.

Category	14.4	Trojans	

### 2004-01-12 Trojan horse malware spoofing masquerade Microsoft update

NIPC/DHS; http://www.gcn.com/vol1\_no1/daily- updates/24599- 1.html

January 09, Government Computer News - New malware masquerades as Microsoft update.

A Trojan horse program that appears to be a Microsoft security update can download malicious code from a remote Web site and install a back door on the compromised computer, leaving it vulnerable to remote control. IDefense Inc., computer security company, said the malicious code is the latest example of so-called social engineering to fool Windows users. It is similar to the W32Swen worm, which last year passed itself off as a Microsoft patch. "The success of Swen in 2003 encouraged virus writers to put effort into creating official-looking e-mails and Web sites," said Ken Dunham, director of malicious code for iDefense. The Trojan arrives as an attachment to an e-mail that appears to be from Windowsupdate@microsoft.com. The subject line says, "Windows XP Service Pack (Express)-Critical Update." The message describes the attachment, WinxpSp1.A, as a cumulative patch that corrects security flaws in versions of Microsoft Internet Explorer, Outlook and Outlook Express. It downloads an executable file that will open a TCP port to listen for remote commands from the attacker.

### Category 14.4 Trojans Trojan horse peer-to-peer P2P software threat Phatbot disable antivirus

2004-03-17

NewsScan

THE PHATBOT TROJAN

The U.S. Department of Homeland Security has alerted computer security experts about the Phatbot Trojan, which snoops for passwords on infected computers and tries to disable firewall and antivirus software. Phatbot, which is a "Trojan horse" because it lets vandals take surreptitious control of unsecured computers, has proved difficult for law enforcement authorities and antivirus companies to fight against. Mikko Hypponen, director of the antivirus software company F-Secure in Finland says, "With these P2P Trojan networks, even if you take down half of the affected machines, the rest of the network continues to work just fine"; security expert Russ Cooper of TruSecure warns, "If there are indeed hundreds of thousands of computers infected with Phatbot, U.S. e-commerce is in serious threat of being massively attacked by whoever owns these networks." (Washington Post 17 Mar 2004)

Category 14.4 Trojans 2004-05-12 **Trojan Horse Mac Apple Applescript** 

DHS IAIP Daily;

http://www.macworld.co.uk/news/top\_news\_item.cfm?NewsID=8665

May 12, Macworld — Trojan is attacking Macs.

Intego has identified a Trojan horse - - AS.MW2004.Trojan - - that affects Mac OS X. This Trojan horse, when double- clicked, permanently deletes all the files in the current user's home folder. Intego has notified Apple, Microsoft and the CERT, and has been working in close collaboration with these companies and organizations. The AS.MW2004.Trojan is a compiled AppleScript applet, a 108 KB self- contained application, with an icon resembling an installer for Microsoft Office 2004 for Mac OS X. This AppleScript runs a Unix command that removes files, using AppleScript's ability to run such commands. The AppleScript displays no messages, dialogs or alerts. Once the user double- clicks this file, their home folder and all its contents are deleted permanently. All Macintosh users should only download and run applications from trusted sources.

Category 14.4 Trojans

#### 2004-05-12 bot zombie Trojan Horse malicious code phatbot

DHS IAIP Daily;

http://www.theregister.co.uk/2004/05/12/phatbot\_zombie\_trade /

May 12, The Register — Phatbot arrest throws open trade in zombie PCs.

The arrest of the suspected author of the Phatbot Trojan Friday, May 7, in the southern German state of Baden- Wuerttemberg could lead to valuable clues about the illicit trade in zombie PCs. The arrest was overshadowed by the unmasking of the admitted Sasser author. But the Phatbot case may shed the most light into the dark recesses of the computer underground. Phatbot is much less common than NetSky but is linked much more closely with the trade in compromised PCs to send spam or for other nefarious purposes. Viruses such as My- Doom and Bagle (and Trojans such as Phatbot) surrender the control of infected PCs to hackers. This expanding network of infected, zombie PCs can be used either for spam distribution or as platforms for DDoS attacks, such as those that many online bookies have suffered in recent months. By using compromised machines- - instead of open mail relays or unscrupulous hosts- - spammers can bypass IP address blacklists. Phatbot is a variant of Agobot, a big family of IRC bots. Networks of compromised hosts (BotNets) are commonly traded between virus writers, spammers and middlemen over IRC networks. The price of these BotNets (DoSNets) was roughly \$500 for 10,000 hosts last summer when the MyDoom and Blaster (the RPC exploit worm) first appeared on the scene.

Category 14.4 Trojans

2004-05-18 worms Trojans blended threats kibuv bobax

DHS IAIP Daily; http://www.eweek.com/article2/0,1759,1594860,00.asp

May 18, eWeek — Kibuv worm, Bobax Trojan try many methods.

Security experts are tracking two new threats that have emerged in the past few days, including a worm that uses seven mechanisms to spread itself. The worm is known as Kibuv, and researchers first noticed its presence Friday, May 14. Kibuv affects all versions of Windows from 98 through Windows Server 2003 and attempts to spread through a variety of methods, including exploiting five Windows vulnerabilities and connecting to the FTP server installed by the Sasser worms. The worm has not spread too widely as of yet, but with its variety of infection methods, experts say the potential exists for it to infect a large number of machines. The second piece of malware that has surfaced is a Trojan that is capable of spreading semi- automatically. Known as Bobax, the Trojan can only infect machines running Windows XP and seems to exist solely for the purpose of sending out large amounts of spam. When ordered to scan for new machines to infect, Bobax spawns 128 threads and begins scanning for PCs with TCP port 5000 open. If the port is open, it exploits the Windows LSASS vulnerability. Bobax then loads a copy of itself onto the new PC, and the process repeats. Antivirus and antispam providers say they have seen just a few machines infected with Bobax as of Tuesday, May 18.

## Category 14.4 Trojans

2004-05-20

## Trojan Horse financial services identity theft online banking

DHS IAIP Daily; http://www.computerworld.com/securitytopics/security/story/0,10801,93281,00.html

May 20, Computerworld — Canadian online banking users fall victim to Trojan.

A Trojan horse may be responsible for an online banking scam that has cost at least two Winnipeg, Canada, customers thousands of dollars. The Winnipeg Police Service is investigating two cases where money was transferred unknowingly from bank accounts. The investigation is focused around a man who recently emigrated to Canada from an unidentified locale in Eastern Europe. According to computer security experts, online banking scams and identity theft are proliferating in Canada. While Canadian e- banking customers have yet to see a surge in identity theft similar to the U.S., the banks say the onus is on consumers and enterprises to protect themselves. Keystroke loggers are the most frequently used tactic for crooks targeting banking information, said Tom Slodichak, chief security officer of WhiteHat, an IT security provider. "Although a Web session with their financial institution is usually encrypted, the keystroke logger intercepts the keystrokes before any encryption occurs, so they will get all the information- - the account numbers, the names, the passwords or PINs or whatever they need to impersonate that [individual]," he said.

Category 14.4 Trojans

## 2004-06-29 network vandals banking information keylogger Trojans

NewsScan

NETWORK VANDALS WANT TO BANK WITH YOU

Computer security experts are issuing warnings that network vandals hope to steal the password and account information of online bank accounts by secretly downloading spy software to capture a PC user's keystroke activity. The problem is not widespread, but Internet Explorer users are being advised to set the security setting for their browsers to "high" (a level which, however, makes it more difficult to interact with some Web sites). (Washington Post 29 Jun 2004)

# Category 14.4 Trojans 2004-08-10 Trojan Horse malicious code peer-to-peer P2P networks Windows Pocket PC Symbian smartphone attack

DHS IAIP Daily; http://www.theregister.co.uk/2004/08/10/mosquitos\_trojaned/

August 10, The Register — Trojan dialler afflicts Symbian smartphones.

Malicious code that dials premium rate numbers without a user's consent has been found in a pirated version of Mosquitos 2.0, a popular game for Symbian Series 60 smartphones. The illicit copies of the game are circulating over P2P networks. News of the Symbian Trojan dialler comes days after the arrival of the first Trojan for handheld computers running Windows Pocket PC operating system, Brador- A.

### Category 14.4 Trojans

2004-10-25 Red Hat Linux patch malicious hoax e-mail SANS message

DHS IAIP Daily; http://searchsecurity.techtarget.com/originalContent/0,28914 2,sid14\_gci1019189,00.html

October 25, SearchSecurity — Red Hat Linux patch update a malicious hoax.

An e- mail disguised as a Red Hat patch update is a fake designed to trick users into downloading malware designed to compromise the systems they run on, the Linux vendor warned in a message on its Website. While the malicious site was taken down over the weekend, the SANS Internet Storm Center posted a message on its Website saying the hoax "is a good reminder that even though most of these are aimed at Windows users, always be suspect when receiving an e- mail asking you to download something."

Category 14.4 Trojans

2004-11-23 trojan mobile phones skulls Nokia Symbian vandalism denial-of-service attack

NewsScan; http://www.enn.ie/news.html?code=9566568

TROJAN HORSE AIMED AT NOKIA CELL PHONES

A new attack by Trojan Horse software known as "Skulls" targets Nokia 7610 cell phones, rendering infected handsets almost useless. It replaces most of an infected phone's program icons with images of skulls and crossbones, and disables all of the default programs on the phone (calendar, phonebook, camera, Web browser, SMS applications, etc.) -- i.e., essentially everything except normal phone calls. Symbian, the maker of the Nokia 7610 operating system, says that users will only be affected if they knowingly and deliberately install the file and ignore the warnings that the phone displays at the conclusion of the installation process. Experts don't consider the Skulls malware to be a major threat, but note that it's the third mobile phone bug to appear this year -- and therefore probably means that this kind of problem is here for the foreseeable future. (ENN Electronic News.net 23 Nov 2004)

### 14.5 Virus hoaxes

Category 14.5 Virus hoaxes

virus hoax Bin Laden suicide al Qaeda terrorism fear uncertainty doubt FUD

2004-07-26 NewsScan

BIN LADEN HOAX VIRUS WARNING

E-mail purporting to contain evidence of Osama bin Laden's suicide contains a "Trojan horse" virus that could allow network vandals to take over infected computers. Naming the new scheme the Hackarmy Trojan horse, the antivirus firm Sophos says, "Thousands of messages have been posted onto Internet message boards and usenet newsgroups claiming that journalists from CNN found the terrorist leader's hanged body earlier this week." The messages point to a site where it's claimed that a file of photographs can be downloaded, but what the file really contains is a Trojan horse that can allow hackers to gain remote control of an infected computer. (The Australian 26 Jul 2004)

### 15.1 Fraud

 Category
 15.1
 Fraud

 2004-01-05
 bribery IBM Korea

DHS/IAIP Update

IBM execs, S. Korea officials accused of bribery

Some 48 South Korean government officials and corporate executives, mainly from IBM ventures, have been charged with bribery in a case involving state contracts for computer parts and servers, prosecutors said Monday. Fourteen government officials were bribed a total of \$240,000 (290 million won) and an IBM Korea executive received golf memberships worth \$82,000 from a subcontractor, prosecutors said. IBM Korea, a unit of IBM, said it did not condone the activities and that it had fired some staff involved in the case.

Category 15.1 Fraud

#### 2004-01-05 fraud internet Operation Cyber Sweep online economic crime

NewsBits; http://www.latimes.com/technology/la-tr-internet4jan04,1,4364631.story

Fraud crackdown highlights fears over booking trips on Web Internet-related crime is a large and growing problem.

More than a third of the 218,000 fraud complaints the Federal Trade Commission received in 2002 were Web-related. In October, the FBI implemented Operation Cyber Sweep, a coordinated nationwide enforcement operation designed to crack down on the leading types of online economic crime. By November, it announced the arrests or convictions of more than 125 people. Investigators discovered more than 125,000 victims, with estimated losses totaling more than \$100 million. (LA Times article, free registration required)

Category 15.1 Fraud

2004-02-04Internet fraud law Congress prison sentences copyright violation intellectual<br/>property rights

NewsScan

CONGRESS TARGETS ONLINE FRAUD

The Fraudulent Online Identity Sanctions Act, sponsored by U.S. Reps. Lamar Smith (R-Texas) and Howard Berman (D-Calif.), would tack as much as seven years on to prison sentences handed down to fraudsters using the Internet to bilk unsuspecting users through a Web site registered under a false name or contact information, and would also allow copyright owners to seek larger monetary damages from fraudulently registered sites that distribute copyrighted material without permission. "The Government must play a greater role in punishing those who conceal their identities online, particularly when they do so in furtherance of a serious federal criminal offense or in violation of a federally protected intellectual property right," says Smith. The proposal could hit a snag if privacy advocates lobby against it, maintaining that private information such as home addresses and phone numbers should not be made available on the public "whois" domain name databases against the registrant's wishes. "Because of the way whois is currently structured, there are a lot of reasons why users might submit false information that have nothing to do with copyright infringement," notes Michael Steffen, a policy analyst at the Center for Democracy and Technology. (Washington Post 4 Feb 2004)

Category15.1Fraud2004-02-12Net-harm Internet assasination hitlist Korea murder Website

NewsScan

MURDER IN THE INFORMATION AGE

In Korea, police have arrested a 25-year-old college senior and charged him with operating a killer-for-hire Web site and taking thousands of dollars from his customers. In one case the student allegedly received the equivalent of \$8,600 from a 22-year-old woman who wanted her ex-boyfriend and his wife murdered; in another there were discussions with a boy who wanted his father and stepmother killed. None of the murder plots was carried out. (AP/USA Today 12 Feb 2004)

### Category15.1Fraud2004-02-25Microsoft fraud cyber crime warning businesses under attack criminals

DHS IAIP Daily;

http://www.computerweekly.com/articles/article.asp?liArticleID=128636&liArticle TypeID=1&liCategoryID=2&liChannelID=22&liFlavourID=1&sSearch=&nPage= 1

February 25, Computer Weekly - Businesses are under attack from cyber criminals, says MS security head.

Businesses worldwide face increasing threats from cyber criminals attempting extortion and fraud because the software running their systems makes them vulnerable, said Microsoft's top security architect at the e- Crime Congress in London. Security architect and chief technology officer of Microsoft's security business unit David Aucsmith admitted that he is considered a "target" for complaints against his company's software, but he also stressed that many of the security issues could not have been foreseen. Microsoft is addressing these security issues by working closely with law enforcement authorities and changing its patching procedures. Much of the threat comes from criminals who are making a career from high- tech crimes such as hacking, extortion and fraud, he said. The time between the release of a patch and the creation of an exploit has dwindled dramatically. Hackers have the advantage of not having to test their exploits, which allows them to move faster than suppliers who must perform rigorous testing to ensure that their patches do not break users' systems.

# Category 15.1 Fraud 2004-03-09 fraud Internet resumes CV curriculum vitae misrepresentation lies background checks hiring

NewsScan

**RESUME FRAUD GOES HIGH-TECH** 

As companies ratchet up efforts to detect misrepresentations on job seekers' resumes, resume fraud is jumping to a new level, thanks to operators of Web sites that provide phony degrees and toll-free numbers for employers to call, where they're assured that a job candidate's credentials are valid. Some candidates are even paying hackers to alter class lists at universities they claim to have attended, says Charles Wardell, managing director at Korn/Ferry International. "In the past, people just lied. Now, what they are doing is they are hacking into a class of a university and putting their name on the class list." Wardell says his company has started requesting degrees and, in some cases, even grades from potential job candidates, but such documents are also easily faked, thanks to the ingenuity of Web sites such as easydiploma.com, which offers phony degrees and a verification service. "You can select the parchment paper, the insignia and the type of degree," says the head of a corporate investigation firm's background screening division. Background search firms say these increasingly sophisticated resume fraud schemes are making their jobs more difficult: "A good liar understands that you have to have some basis and facts to pull off a scam. But it's even more dangerous when employers unknowingly hire a fraud, thief or a crook," says the president of Employment Screening Resources.

### Category15.1Fraud2004-03-104-1-9 Nigerian advance fee fraud swindler stupidity

http://www.theregister.co.uk/2003/03/10/419\_scammers\_take\_us\_con/

The Register published the following summary of a hilarious tale of stupidity and cupidity:

>419 SCAMMERS TAKE US CON ARTIST FOR \$750,000 By Lester Haines Published Monday 10th March 2003 15:07 GMT

A businessman in Winona, Minnesota, has been taken for a cool \$750,000 by Nigerian 419 scam artists, the Winona Daily News reports.

Nothing new there, you might think, but \$250,000 of the cash did not actually belong to victim Carl Fratzke. Incredibly, Fratzke had pulled a scam of his own and defrauded seven friends to raise the capital. The balance came from his own savings.

Tempted, as ever, by promises of riches beyond the wildest dreams of avarice, Fratzke asked chums to invest in a scheme whereby he would buy gloves and sell them to Wal-Mart at a hefty profit. He promptly sent the cash straight to the 419 scammers.

"They sent me a facsimile of the check they were going to send me," Fratzke later testified before a presumably astounded judge. "They said: "This is coming'."

Well, it didn't, and now Fratzke faces sentencing on 31 March on "two counts of theft by swindle and one count of theft by check". If he's lucky, the beak will hand down a stiff sentence. Jail is probably the only place he'll be safe from his friends and investors — and his own stupidity.<

Category 15.1 Fraud

#### 2004-03-31 fraud confidence game swindle Nigerian 4-1-9 advance-fee fraud

http://www.boston.com/news/local/massachusetts/articles/2004/03/31/man\_arr ested\_in\_alleged\_investment\_scam/

John Paczkowski, writing his column "Good Morning Silicon Valley" in the Silicon Valley Mercury News, wrote the following succinct summary of a tragic tale:

>...[F]ormer Dana-Farber Cancer Institute researcher and Harvard University professor. Weldong Xu, an academic who had done stints at both hallowed institutions, was arrested yesterday and charged with bilking friends and colleagues out of some \$600,000 and then investing it in a questionable Nigerian business venture from which he expected a \$50 million return. Xu allegedly persuaded a total of 35 people since last July to give him money, telling them it was for researching severe acute respiratory syndrome, before handing it over to the 419ers. "I tried to tell him he had been scammed," said Detective Steve Blair. "His plan all along was this Nigerian investment."<

<http://www.mercurynews.com/mld/siliconvalley/business/columnists/gmsv/8321286.htm?1c>

Category 15.1 Fraud

2004-04-27 UK cybercrime law review organized crime gangs hacking spam virus-writing

DHS IAIP Daily; http://www.cnn.com/2004/TECH/internet/04/27/crime.britain.in ternet.reut/index.html

April 27, Reuters — UK to review cybercrime law.

Britain is to update its lone cybercrime law. Organized gangs around the world are honing their hacking, spamming and virus- writing skills while thinly stretched police resources are struggling to cope. The legal update will be closely watched by other countries, many of whose own laws against cybercrime are considered insufficient to fight what has become one of the fastest growing global crime waves. A group of parliamentarians will hold a public debate on Thursday, April 29, to explore ways to bring the Computer Misuse Act, or CMA, into the Internet era. Working with the UK's Home Office, the aim is to have a new cybercrime bill introduced in the next six months, MP Brian White said. Police say cybercrime costs UK industry hundreds of millions, and perhaps billions, of pounds annually. Globally, the figure is staggering, law enforcement officials say. "Serious and organized crime groups, and potentially terrorists, are moving into cyberspace simply because it's easier to hide there," said Simon Moores, a computer crime expert who works with the UK government. Thin resources, few convictions The need for an updated law is most evident to prosecutors and police. The Home Office said there were just 14 convictions under the CMA in 2002, the last year statistics were tallied.

Category 15.1 Fraud

2004-04-29 fraud data mining banking FinCEN

DHS IAIP Daily; http://www.gcn.com/vol1\_no1/daily- updates/25782- 1.html

April 29, Government Computer News — Financial Crimes and Enforcement Network plans to modernize Bank Secrecy Act database.

The Department of Treasury's Financial Crimes and Enforcement Network (FinCEN) plans to update its computer database next year with a new data retrieval system, along with applications that will perform deeper analysis and improve data- mining capabilities. Banks report suspicious activity and other data through FinCEN's Patriot Act Communications System, including when customers make unusually large deposits or withdrawals. Law enforcement agencies can access and download the confidential information in FinCEN's database to help uncover and track terrorist financing. Bank Secrecy Act (BSA) Direct, which is basically a data warehouse, will make the information more easily accessible and understandable to law enforcement while securing the information from unauthorized users, according to FinCEN director William Fox.BSA Direct will also alert FinCEN to irregularities in Bank Secrecy Act reports submitted by financial institutions, and will audit use of the accessed data to ensure that it is not misused, Fox said. A networking function will link different law enforcement entities that are accessing the same data to avoid overlap or conflict in investigations. FinCEN expects to have BSA Direct online in the fall next year, Fox said.

Category 15.1 Fraud

#### 2004-05-17 fraud online job listings identity theft credit card theft

DHS IAIP Daily; http://www.nytimes.com/2004/05/17/technology/17ecom.html

May 17, New York Times — Fraud in online job listings.

Online job sites like Monster.com, CareerBuilder and HotJobs have given employers another way to find workers, but it turns out that crime rings are making use of the sites, too. In a recent swindle, for instance, credit card thieves found unwitting money launderers through Monster.com, then left their "employees" on the hook for thousands of dollars in debts and possible criminal liability when the fraud was discovered. Federal authorities said the recent swindle was one they had not yet seen. Molly S. McMinn, an inspector for the United States Postal Inspection Service said this type of fraud was "a new twist on an old idea" of credit card thieves from foreign countries buying merchandise from online merchants with card numbers stolen from American citizens and having the merchandise shipped to associates in the United States. McMinn said fraud rings would recruit associates by putting ads on job sites for "reshippers," who, in exchange for a fee, mail the merchandise to Ukraine, Indonesia or other countries known by online merchants as hotbeds of Internet fraud. By using middlemen based in the United States, criminals can escape detection by merchants.

Category 15.1 Fraud

#### 2004-05-27 ATM scam casino organized crime theft fraud

DHS IAIP Daily;

http://www.lasvegassun.com/sunbin/stories/lv- crime/2004/may/27/516925888.html

May 27, Las Vegas Sun — Eleven sought in ATM, casino scam.

The FBI continues to search for 11 people named in two federal racketeering indictments alleging two Romanian crime rings are using stolen credit cards and false identification to bilk hundreds of thousands of dollars from Las Vegas, NV, casinos and ATMs. The indictments allege the credit card rings sent out runners across the country to steal credit cards that were then transported to Las Vegas, where they were used with fake driver's licenses to obtain cash advances at casinos and from automated teller machines. The groups liked to prey on people at fitness centers, where credit cards were easily taken from lockers while people worked out, or from cars parked at trail heads at recreation areas, Assistant U.S. Attorney Tim Vasquez said. On Tuesday, May 25, the FBI seized computers, printers, digital cameras, lock- picking tools, laminators, credit cards, ATM components and an ATM from the Las Vegas homes of the six people arrested in Las Vegas. "We believe they used the ATM machine to practice one of their newer techniques, which was using skimming devices," Vasquez said.

Category15.1Fraud2004-06-02Internet scam fraud John Grisham novel plot "The Brethen"

NewsScan

INTERNET SCAM FOLLOWS PLOT OF GRISHAM NOVEL

"I think the public needs to be protected from you," U.S. District Judge Ellen B. Burns told Steven Smith, a Connecticut man who posted Internet personal ads in which he pretended to be a gay man rejected by his parents and looking for guidance from older men. When men responded to the ads Smith told them he was in jail and needed money to be released. The scam echoes the plot of a John Grisham novel called "The Brethren," in which the perpetrators of a similar scam unknowingly ensnare a presidential candidate, from whom they then attempt to extort money as he gains front-runner status. (AP/USA Today 2 Jun 2004)

Category 15.1 Fraud

2004-06-04 Nigerian 4-1-9 scam software Nigeria government catch banking petroleum industry

NewsScan

NIGERIA MAY USE SOFTWARE TO NAB SCAMMERS

Nigeria plans to launch software that will search for certain keywords to help catch fraud perpetrators who send scam letters via e-mail. Nigerian official Mustafa Bello explains: "The introduction of new software, currently under discussion within the Nigerian parliament, will scan e-mails originating in Nigeria to look for keywords commonly found, especially relating to banking and the country's petroleum industry. This will then be removed from the system and even traced back to where it originated." (The Age 4 Jun 2004) Rec'd from John Lamp, Deakin U.

Category 15.1 Fraud

#### 2004-07-29 extortion fraud Russia British bookmaker denial-of-service threat e-mail

NewsScan

RUSSIAN EXTORTIONISTS: EACH DID HIS BIT OF WORK

Police authorities in Russia have broken up a hacker ring that extorted money from British bookmakers by flooding online betting sites with false requests for information in "denial-of-service" attacks and then sending e-mail demanding money for stopping the attacks. Investigators said that

bookmaker companies were the most convenient prey because the attacks could be timed to major sport events. The ring consisted of well-educated people in their early 20s who had found each other on the Internet and agreed to work together in the extortion. A Russian police official said: "There was no chief organizer in plain terms, each of them did his bit of work. And they didn't consider themselves criminals." (AP 29 Jul 2004)

Category 15.1 Fraud

#### 2004-08-26 Internet crime identity theft hacking phishing Operation Web Snare

DHS IAIP Daily;

http://story.news.yahoo.com/news?tmpl=story2&u=/nm/20040826/ wr nm/crime internet dc

August 26, Reuters — U.S. says over 100 arrested in Internet crime sweep.

More than 100 people have been arrested in the largest global crackdown to date on identity theft, hacking and other Internet- based crimes, Attorney General John Ashcroft said on Thursday, August 26. The arrests followed a three- month investigation into a range of crimes from reselling co- workers' Social Security numbers to disabling Websites, Ashcroft said. The crackdown, dubbed "Operation Web Snare" cost some 150,000 victims more than \$215 million, Ashcroft said, adding that 53 people had already been convicted. Phishing, the sending of e- mails designed to look like they are from legitimate financial institutions, and identity theft were two of the major schemes targeted. Law enforcement officials in Romania, Nigeria and Cyprus helped track down people involved in fraudulent auctions, trafficking in stolen credit card numbers and other crimes, Ashcroft said.

### Category 15.1 Fraud

2004-10-05 e-mail scam fraud US elections Czech Republic origin

DHS IAIP Daily; http://news.bbc.co.uk/1/hi/technology/3714944.stm

October 05, BBC News (UK) — E- mail scam plays on U.S. elections.

People are being warned about a scam e- mail which uses the U.S. presidential poll to con them out of their money. A junk e- mail invites people to dial a premium rate number to express their support for President George W. Bush or Senator John Kerry. E- mail filtering firm BlackSpider estimates that almost a quarter of a million are being sent out every day. BlackSpider Technologies said it had traced some of the e- mails to a server in the Czech Republic. "This is a relatively new scam," said BlackSpider CEO, John Cheney.

# Category 15.1 Fraud 2004-11-11 bride Russia e-mail prosecution trial suspended sentence dating cybersex seduction 4-1-9 Nigerian scam

NewsScan; http://theage.com.au/articles/2004/11/11/1100131119740.html

ONLINE BRIDE SCAM

A Russian man who netted \$300,000 by faking emails from prospective brides to unsuspecting foreigners was caught by Moscow police but received only a one-year suspended sentence. Yury Lazarev, 34, an English translator from the Urals, employed women to write flowery, romantic messages signed with real names picked off web dating sites. The photographs of seductive women that accompanied the text caught the attention of some 3000 men from New Zealand, Australia, Canada, the United States and other countries. Once a prospective victim got interested and wanted to meet his potential fiancé, the fictitious woman would ask for financial help in paying for visas and airline tickets. (The Age 11 Nov 2004)

[MK notes: this is a variant of the notorious "Nigerian 4-1-9" or "advance-fee" fraud.]

Category 15.1	Fraud
2004-12-15	US Time Warner AOL SEC Securities Exchange Commission fraud accounting civil lawsuits criminal prosecution settlement

NewsScan; http://www.nytimes.com/2004/12/15/business/media/15media.html

U.S. AND TIME WARNER: LET'S SETTLE UP

Time Warner has agreed to settle with the government in two separate cases: the Justice Department's investigation of whether AOL's advertising deals with smaller Internet companies were used to exaggerate AOL growth, and the SEC's investigation into accounting irregularities at the company. Time Warner is expected to pay \$500- 600 million to settle all civil and criminal accusations with the two agencies. (New York Times 15 Dec 2004)

### 15.2 Extortion

Category	15.2	Extortion		
2004-02-2	26	data theft extortion Japan arrest customer information organize	ed crime	
RISKS			23	22
4.6-MILL	ION DSL SUE	SCRIBERS' DATA LEAKED IN JAPAN		
Tokyo Me	tropolitan Poli	ce arrested three meno n suspicion of trying to extort up to 3 billion yen (U.S.	. \$28 million) f	from

Softbank. The suspects claimed that they obtained DVD and CD disks filled with 4.6 million Yahoo BB customer information. Two of the suspects run Yahoo BB agencies which sells DSL and IP Telephone services.... According to Softbank, the stolen data includes name, address, telephone number, and e-mail. No billing or credit card information was leaked. However, there were indications that the suspects could be linked to organized crime (the Yakuza).

Category 15.2 Extortion

2004-03-20 extortion fraud spoofing advertising software malware arrest arraignment trial

http://www.siliconvalley.com/mld/siliconvalley/8234511.htm

COMPUTER PROGRAMMER ARRESTED FOR EXTORTION AND MAIL FRAUD SCHEME TARGETING GOOGLE, INC.

Extracts from the press release from the US Department of Justice, March 18, 2004

The United States Attorney for the Northern District of California announced ... that Michael Anthony Bradley, 32, of Oak Park, California, was arrested ... [on March 17] on a criminal complaint filed in San Jose charging him with interfering with commerce by threats or violence in violation of 18 U.S.C. § 1951, and mail fraud in violation of 18 U.S.C. 1341....

According to the criminal complaint, which was unsealed in San Jose today, Mr. Bradley attempted to defraud and extort money from Google, the Internet company best known for its free search engine, by developing a software program that automates fraudulent "clicks" on "cost-per-click" advertisements utilized by Google. These fraudulent clicks, in turn, were designed to cause Google to make payments that were supposed to be made only for "clicks" made by legitimate Web surfers.

The complaint alleges that Mr. Bradley first sent an email requesting a meeting with Google concerning his software program, which he named Google Clique, in early March. In a subsequent face-to-face meeting with Google engineers on March 10, the complaint alleges that Mr. Bradley performed a demonstration of his program, and claimed that it generated false clicks that look like real Internet traffic and were untraceable. The defendant allegedly stated that he would sell it to top spammers if Google did not pay him \$100,000, and that Google would lose millions.

The maximum statutory penalty for each violation of 18 U.S.C. \$ 1341 and 1951 is 20 years imprisonment and a fine of \$250,000..."

Category 15.2 Extortion

2004-03-23 computer crime threat Google California

NewsScan

THREATEN GOOGLE, GET ARRESTED

Federal law enforcement officials in California have arrested a 32-year-old man who demanded \$100,000 from Google Inc. and threatened to "destroy" the company by using a a software program to fake traffic on Internet ads. The man's program automated phony traffic to cost-per-click ads Google places on websites and caused Google to make payments to Web sites the man had set up. Released on \$50,000 bail, he faces up to 20 years in prison and a \$250,000 fine. (Bloomberg News/Los Angeles Times 23 Mar 2004)

### Category15.2Extortion2004-05-26organized crime fraud identity theft extortion

DHS IAIP Daily:

http://www.theage.com.au/articles/2004/05/26/1085461818627.h tml

May 26, Australian Associated Press — Mobsters targeting Australians online.

Australians are being targeted by Eastern European organized crime families using the internet to extort and steal far from home. Delegates at the annual AusCERT Asia Pacific Internet Security Conference were warned Wednesday, May 26, that mobsters were hiring computer programmers to take their brand of criminal activity online. The deputy head of Britain's National Hi- Tech Crime Unit, Superintendent Mick Deats, said one Eastern European syndicate with interests in prostitution, drugs and gun smuggling was also earning money all over the world from internet credit card fraud, software piracy, child pornography and online extortion. "Australia is a focus of a lot of the phishing activity at the moment," Deats said. "The people we've arrested in London were sending money to the same people that are receiving money from attacks that are happening in Australia." Another tactic linked to several eastern European crime syndicates was using distributed denial of service attacks - bombarding online businesses with a flood of requests aimed at overloading systems and shutting them down. The businesses were then told to pay \$50,000 to make the attacks go away, he said.

Category 15.2 Extortion

#### 2004-05-31 extortion fraud Softbank Tokyo database right-wing extremist

NewsScan

ARRESTS OVER SOFTBANK EXTORTION

Police have arrested two additional people on suspicion of trying to extort money from Softbank after obtaining personal data on as many as 4 million subscribers to the Internet company's broadband service. The two -- Yutaka Tomiyasu, 24, and Takuya Mori, 35 -- are accused of obtaining company passwords to hack into Softbank's database from an Internet cafe in Tokyo in January, according to a Tokyo Metropolitan Police spokesman. The two allegedly passed the information to members of a rightwing extremist group, police said. Four members of the extremist group were arrested in February for allegedly threatening to publicly release the information

unless Softbank paid them ¥1 billion to ¥2 billion (\$US13 million to \$US26 million). (The Australian 31 May 2004) rec'd from John Lamp, Deakin U.

# 16.2 Industrial information systems sabotage

Category	16.2	Industrial information systems sabotage		
2004-02-1	19	information warfare quality assurance QA Trojans bad code		
RISKS; h	ttp://seclists.	org/lists/isn/2004/Feb/0011.html	23	21
MALICIC	US IT DESIG	N IN SUPPORT OF THE COLD WAR		

Sam Garst contributed this abstract to RISKS:

On 2 Feb 2004, \*The New York Times\* printed an editorial by William Safire entitled "The Farewell Dossier" describing a CIA campaign in the early 1980s that supplied Russia with deliberately flawed technology; this lead directly to the massive explosion of a Siberian gas pipeline. The CIA became aware that the KGB was purchasing technology on the black market, and endeavored to supply the KGB with technology that would pass inspection, and later fail catastrophically.

Two risks leap out at me (trying hard to separate out several moral issues):

- I may test for poor design, or poor manufacturing, but these products were designed to pass testing, and then fail. Should I start testing for malicious design (perhaps, if you're building sensitive infrastructure, this is common practice)?

- These intentional flaws could 'leak' into the legitimate product lines. Hopefully, these companies had (and still have) good software build processes and code repositories...

Safire indicates the story is from a soon-to-be published book: Thomas C. Reed's \_At the Abyss\_

# 16.3 Infrastructure protection & homeland security

Category 16.3 Infrastructure protection & homeland security

#### 2004-01-08 US government IT security efforts department

NIPC/DHS; http://www.eweek.com/article2/0,4149,1426312,00.asp

January 05, eweek.com — Agencies beef up IT security.

The Department of Justice (DOJ), one of a handful of agencies that received a failing grade on last month's report card on IT security delivered by a congressional subcommittee, is at the forefront of the movement. The DOJ has made a number of changes, including the establishment of a department-wide IT security staff that answers directly to the CIO, according to DOJ officials. That group, in turn, has set about organizing a security council within the department, they said. The council comprises the top security officials from each of Justice's dozens of component organizations, and is now responsible for implementing and overseeing all the security programs in the department. So far, the results have been encouraging, department officials said. Another agency, the Environmental Protection Agency has created an automated security evaluation and remediation application capable of testing the security posture of each machine and monitoring the remediation process for any problems found. The Department of Transportation recently implemented a comprehensive vulnerability assessment and remediation package that performs continuous scans, instead of the traditional monthly or quarterly assessments.

Category 16.3	Infrastructure protection $\&$ homeland security
2004-01-09	Homeland Security terrorism anti-terrorism flight cancellation airline plane fear uncertainty doubt FUD

RISKS

13

23

#### BRUCE SCHNEIER ON ORANGE ALERT IN SALON (FROM DAVE FARBER'S IP)

Contributor Cory Doctorow supplies a Bruce Schneier article on flight cancellations and US anti-terrorism efforts. In this article entitled "Homeland Insecurity," Schneier analyzes the event of 15 flight cancellations in the US in January 2004. Schneier points out that all 15 of these flight cancellations had turned out to be false alarms. He says that security is a tradeoff between its costs and benefits, and stresses that cancelling flights because of not-so-credible threats will be too expensive in the long run. But Schneier appreciates that intellegence is difficult, and involves painstaking data analysis. "The crucial bits of data," he observes, "are just random clues among thousands of other random clues, almost all of which turn out to be false or misleading or irrelevant." He says that, in fact, working with too much data can be problematic. Schneier adds that throwing more computers into data analysis will not help because "[F]inding the real plot among all the false leads requires human intelligence." He concludes that the 15 airline cancellations reflected old problems with US intelligence--"too much bureaucracy and not enough coordination."

 Category 16.3
 Infrastructure protection & homeland security

 2004-01-18
 quality assurance vendor liability Department Homeland Security DHS software products support anti-terrorism by fostering effective technology SAFETY quality anti-terrorism technology QATT

#### RISKS 23 14 DHS PROTECTS VENDORS OF ANTI-TERRORISM TECHNOLOGIES FROM LIABILITY

Jay Wylie is concerned that Support Anti-terrorism byFostering Effective Technologies (SAFETY) Act of 2002 will lead to worse software-product quality. SAFETY "protects vendors of anti-terrorism products that have been vetted by the Department of Homeland Security and designated as QATT (Qualified Ani-Terrorism Technology) from liabilities that arise from any failings of the anti-terrorism technology," writes Wylie. An article about SAFETY, by Roland L. Trope, appeared in IEEE Spectrum in January 2004. Jay Wylie is dissappointed that this publication by a society of professional engineers "is more concerned about vendors being aware of the protection from liability than questioning whether such protection is appropriate."

Category 16.3	Infrastructure protection & homeland security
2004-01-20	eyeglass lie detector law enforcement airport security anti-terrorism Homeland Security

RISKS; http://www.eetimes.com/story/OEG20040116S0050 23 14 LIE-DETECTOR GLASSES, 90% ACCURATE?

Steve Holzworth refers us to a story in eetimes.com on a new lie-detector technology that may come to be used for airport security soon. This lie detector measures the frequency range of voice patterns to report with 89% accuracy if someone is lying. The lie detector is so small that it can fit in the eyeglasses of law enforcement officers. When an airport security screener asks a passenger, "Do you plan on hijacking this plane?", the lie detector will flash green, yellow, or red to the security screener to indicate true, uncertain, or false passenger responses. Given the success rate of this lie-detector, Steve Holzworth remarks, "Oh, excellent! I only have a 1 in 10 chance of being falsely accused." In a follow-up article, contributor Ron Bean says that this liedetector technology "sounds like it's detecting people's emotional "hot buttons", rather than lies per se." He thinks a good actor could defeat this lie-detector. He concludes by asking, "What's the rate for false positives vs false negatives?" for this liedetector. Contributor Peter B. Ladkin attempts to answer that in his follow-up article. Ladkin says the 89% accuracy of the lie detector says nothing about the technology's usefulness. Ladkin calls false positives and false negatives Type 1 and Type 2 errors respectively. He writes that in order to understand the problem, one needed "reliable information about the background rate of lying" of the population. Ladkin considers three cases with the given 1 in 10 success rate. In the first case, the background rate of lying is 1 in 10; therefore the passenger is never falsely accused of lying. In the second case, all errors are of Type 1; so the passenger "has a 1 in 10 chance of being falsely accused." In the third case, "[E]rrors are evenly split between Type 1 and Type 2, and the background rate of lying is 1 in 2." Now, an innocent passenger and an actual hijacker have a 1 in a 20 chance of failing and passing the test respectively. Ladkin thinks this technology is "impossible in serious use." He concludes, "...the company spokesman is Bsing,

as are most people who claim to have measured the accuracy of lie-"detector" apparatus."

Category 16.3	Infrastructure	nrotection &	homeland security	,
Callgoly 10.0	masnucuit	protition &	nomiciana sciurity	(

#### 2004-01-28 Homeland Security government centralized alert system

NewsScan

#### HOMELAND SECURITY DEPARTMENT TO GIVE CYBER ALERTS

The cyber security division of the Department of Homeland Security is creating a new, centralized system for alerting the country to network threats by providing a clearinghouse of information on hacking, viruses, worms and other forms of cyber terrorism. Cyber security director Amit Yoran explains: "We are focused on making the threats and recommended actions easier for all computer users to understand, prioritize and act upon. The vendor community is focused on sales as well as on protecting their clients. Coming from the U.S. government, the focus [of the new centralized system] is solely on the public interest." (Washington Post 28 Jan 2004)

Category 16.3 Infrastructure protection & homeland security

#### 2004-01-30 IT security funding attention US government

NIPC/DHS; http://www.gcn.com/vol1\_no1/daily- updates/24775- 1.html

January 28, Government Computer News — Davis, Putnam ratcheting up IT security oversight.

Two key lawmakers are pressing agencies to correct longstanding IT security problems. Tom Davis, chairman of the House Government Reform Committee, on Tuesday, January 27, said his committee will hold a hearing this spring on at least two contracts that failed to take the Federal Information Security Management Act into account. Adam Putnam, chairman of the Government Reform Subcommittee on Technology, Information Policy, Intergovernmental Relations and the Census, said he sent a letter to agency secretaries requesting a meeting with their CIOs to discuss their IT security action plans. Putnam said the letters are part of an effort to increase awareness of agency IT security problems. Putnam said his staff already has met with six CIOs and will meet with the CIO Council in March to discuss agency IT security plans, milestones and his subcommittee's expectations. He added his staff also will meet with the appropriations committee staff members to discuss the importance of funding IT security. "We've had some very positive discussions with the CIOs so far," Putnam said.

# Category 16.3 Infrastructure protection & homeland security 2004-03-22 security crisis co-ordination center National Cyber Partnership Homeland Security NIDC (DUS)

#### NIPC/DHS

March 18, Federal Computer Week — Security groups call for crisis coordination center.

Two national task forces organized by the National Cyber Security Partnership on Thursday, March 18, called for a public awareness campaign, an early warning contact network and a national crisis coordination center to improve the nation's responses to cyber vulnerabilities, threats and incidents. Establishing a national crisis coordination center by 2006 most likely would require legislation or an executive order. Guy Copeland, who led the Early Warning Task Force, said the center would coordinate threat analyses, warnings, research and responses for critical infrastructure- sector experts and federal, state and local officials. The early warning contact network, to be set up as early as December, would be a multichannel network housed and administered by the Department of Homeland Security's U.S. Computer Emergency Readiness Team. Communication would occur primarily via the Internet, although task force leaders recommended having a backup means of communicating if the Internet goes down. Reaching home users will be accomplished largely through the cooperation of Internet service providers who would keep their customers informed of cybersecurity threats and attacks, task force leaders said. 2004-03-30 16.3 March 30, SearchSecurity.com — SCADA security hearing begins today. Last summer's massive blackout in the Northeast demonstrated the vulnerability of our nation's most critical networks. It also set in motion an inquiry that today, March 30, brings together legislators and IT experts to discuss how to better secure these networks from further disaster. Supervisory Control and Data Acquisition (SCADA) systems, associated with power plants and other mission- critical networks, especially need stronger protection. "Historically, there is a false sense of security related to SCADA systems. Some administrators have been comforted by the thought that these systems are specialized and often deployed in a 'closed' network utilizing proprietary protocols," explains Andre Yee, president and CEO of a network security vendor. One problem with securing SCADA is the unique nature of the systems. Most operate in real time and can't afford to be offline for lengthy upgrades or security installations, for fear of a degradation of performance. Another problem, Yee notes, is with newer SCADA systems incorporating more Web accessibility, which poses myriad problems when using the Internet, a public conduit susceptible to attack. They also leverage Unix and Windows systems, which puts networks at risk, particularly given the number of vulnerabilities that can be exploited.

Category 16.3 Infrastructure protection & homeland security

2004-03-26 security education coding programming Department Homeland Security

#### DHS IAIP Daily;

March 25, Federal Computer Week — Security needs better education for programmers.

Dealing with Internet computer worms and viruses requires a long- term education effort aimed at programmers while they are still in college, a Department of Homeland Security (DHS) executive said Thursday, March 25. Lawrence Hale, deputy director of the DHS' U.S. Computer Emergency Readiness Team, said, "the things that are costing us the most pain are preventable." Programmers can be taught to avoid creating buffer overflows and other well- known vulnerabilities found in commercial software, said Hale, speaking at the FOSE conference on government technology in Washington, DC. It could be years before the results of education show up in software that is being sold, but the effort is needed more than ever because the problem is getting worse, officials said. Hale said an increasing number of cyberattacks are done for profit. "Worms are turning machines into mail servers," he said. "Your machines are being used to spam." In addition to working with universities to promote secure programming practices, DHS is working with researchers at Lucent Technologies' Bell Labs and other organizations on new tools that could detect the precursors of network attacks, Hale said.

Category 16.3 Infrast	tructure protection $\&$ homeland security
0.0	

2004-03-30 identification authentication airport security lawsuit

NewsScan

ADVOCATE LOSES SUIT AGAINST AIRLINE ID REQUIREMENT

John Gilmore, a privacy advocate with the Electronic Frontier Foundation, has lost a federal lawsuit he'd filed after he'd been denied entry to a Southwest Airlines flight for refusing to show identification prior to boarding. Judge Susan Illston ruled that that a request for a passenger's identification does not violate that passenger's Fourth Amendment rights, and rejected Gilmore's claims that the somewhat vague regulations violated due process. But Gilmore could still find good news in the dismissal of his lawsuit: "Judge Illston confirmed I do have standing to challenge but said, 'You're in the wrong court.' I need to go to the court of appeals. I will continue working on the issue. This isn't the end." (AP/San Jose Mercury News 30 Mar 2004)

### Category16.3Infrastructure protection & homeland security2004-03-30SCADA security hearing power failure blackout Northeast critical infrastructure<br/>protection

DHS IAIP Daily; http://searchsecurity.techtarget.com/originalContent/0,28914 2,sid14\_gci957331,00.html

March 30, SearchSecurity.com — SCADA security hearing begins today.

Last summer's massive blackout in the Northeast demonstrated the vulnerability of our nation's most critical networks. It also set in motion an inquiry that today, March 30, brings together legislators and IT experts to discuss how to better secure these networks from further disaster. Supervisory Control and Data Acquisition (SCADA) systems, associated with power plants and other mission- critical networks, especially need stronger protection. "Historically, there is a false sense of security related to SCADA systems. Some administrators have been comforted by the thought that these systems are specialized and often deployed in a 'closed' network utilizing proprietary protocols," explains Andre Yee, president and CEO of a network security vendor. One problem with securing SCADA is the unique nature of the systems. Most operate in real time and can't afford to be offline for lengthy upgrades or security installations, for fear of a degradation of performance. Another problem, Yee notes, is with newer SCADA systems incorporating more Web accessibility, which poses myriad problems when using the Internet, a public conduit susceptible to attack. They also leverage Unix and Windows systems, which puts networks at risk, particularly given the number of vulnerabilities that can be exploited.

#### Category 16.3 Infrastructure protection & homeland security

#### 2004-03-31 critical infrastructure protection challenges efforts report

NIPC/DHS; http://www.gao.gov/highlights/d04354high.pdf

March 15, General Accounting Office — GAO- 04- 354: Critical Infrastructure Protection: Challenges and Efforts to Secure Control Systems (Report).

Computerized control systems perform vital functions across many of our nation's critical infrastructures. For example, in natural gas distribution, they can monitor and control the pressure and flow of gas through pipelines. In October 1997, the President's Commission on Critical Infrastructure Protection emphasized the increasing vulnerability of control systems to cyber attacks. The House Committee on Government Reform and its Subcommittee on Technology, Information Policy, Intergovernmental Relations and the Census asked GAO to report on potential cyber vulnerabilities, focusing on (1) significant cybersecurity risks associated with control systems (2) potential and reported cyber attacks against these systems (3) key challenges to securing control systems and (4) efforts to strengthen the cybersecurity of control systems. GAO recommends that the Secretary of the Department of Homeland Security (DHS) develop and implement a strategy for coordinating with the private sector and other government agencies to improve control system security, including an approach for coordinating the various ongoing efforts to secure control systems. DHS concurred with GAO's recommendation. Highlights: http://www.gao.gov/highlights/d04354high.pdf

# Category 16.3 Infrastructure protection & homeland security 2004-04-01 Transporation Security Administration TSA RFID tags airplane boarding terrorism anti-terrorism

NewsScan

TSA EYES RFID BOARDING PASSES

The Transportation Security Administration is looking into the possibility of using RFID-tagged airline boarding passes that would enable passenger tracking in airports -- a proposal that has raised the hackles of some privacy advocates. TSA says it would use the special boarding passes in conjunction with its "registered traveler" program, which would permit frequent fliers to provide detailed personal information, corroborated by a background check. The RFID passes would allow these registered travelers to speed through "special lanes" during the boarding process. The TSA has already started work to deploy RFID boarding passes in some countries in Africa under the Federal Aviation Administration's Safe Skies for Africa Initiative. But Katherine Albrecht, who worked against the use of RFID tags on retail goods, says this new proposal is a "nightmare scenario," which uses technology to invade people's privacy. "Are they going to track how long I spend in the ladies room?" she asks. (Computerworld 1 Apr 2004)

2004-04-09
Category 16.3

#### NewsScan

AUSTRALIA DEPLOYS FRAUD-DETECTING PASSPORT SCANNERS

Australia has installed 400 iA-thenticate document readers from Imaging Automation in its airports in the hope of authenticating the passports of every person entering the country. The shoebox-sized device uses multiple light sources to examine hundreds of security features on travel documents. Many of the features, such as the composition of the ink used, are invisible to the naked eye. The iA-thenticate system ranges from \$5,000 to \$15,000 per unit and is being used or tested by a number of countries, including Canada, Hungary, Sweden, Finland and Nigeria. Imaging Automation is marketing the system to the U.S. Department of Homeland Security, which is facing delays in deployment fingerprint and facial biometric systems for passport-authentication. (AP 9 Apr 2004)

Category	16.3	Infrastructure protection & homeland security	
----------	------	---	--

#### 2004-04-21 Department Homeland Security coordination infrastructure protection

DHS IAIP Daily; http://www.informationweek.com/story/showArticle.jhtml?artic leID=18902167

April 19, InformationWeek — DHS needs public- private cooperation.

Speaking at the Information Security Decisions conference in New York on Monday, April 19, Amit Yoran, director of the Department of Homeland Security's National Cyber Security Division, noted the challenges associated with this need for public- sector agencies and private- sector companies to coordinate their knowledge of cyberthreats and physical threats, as well as infrastructure vulnerabilities. DHS estimates that private- sector companies run 85% of the services required to ensure national security, public health and safety, and economic stability. Yet private- sector executives are reluctant to provide critical infrastructure information about their companies' operations for fear of their vulnerabilities becoming a matter of public record. Software quality is also a key issue for cybersecurity- - particularly because most software users aren't security experts. Developers must address the most obvious problems. "Ninety- five percent of software bugs are caused by the same 19 programming flaws," Yoran said. And software quality will only become more difficult to police as more and more is developed by foreign nationals both offshore and within the United States, Yoran said. Companies will have to be on guard against backdoors potentially written into software that could allow access to their systems.

Category 16.3 Infrastructure protection & homeland security

2004-04-25 security clearinghouse Federal government ISACS secure network operations center SOC DHS

DHS IAIP Daily; http://www.eweek.com/article2/0,1759,1572951,00.asp

April 25, eWEEK — Feds making plans for security clearinghouse.

The federal government is developing plans for a secure network operations center (SOC) for all security information flowing to and from the government. The SOC would be a clearinghouse that gathers and analyzes data from the private sector, mainly the Information Sharing and Analysis Centers (ISACS) in several major vertical industries. The SOC would be run jointly by personnel from the DHS and a civilian contractor that would help build the facility. DHS officials said that even though there are less formal information- sharing efforts between government and private industry, there still is a need for a more structured program. "We're trying to operationalize the public/private partnership," said Amit Yoran, director of the National Cyber Security Division at DHS, last week. "The private sector genuinely wants to make progress on this. I think, as we get more considerate of the private sector in terms of the FOIA [Freedom of Information Act] exemption, things will come along." Officials said they hope to have plans for the SOC finalized soon and intend to fund the initiative out of the current fiscal year's budget, which runs out September 30.

### Category16.3Infrastructure protection & homeland security2004-04-27Islamic webmaster free speech trial prosecution civil liberties USAPATRIOT<br/>antiterrorism law

 $\label{eq:http://www.nytimes.com/2004/04/27/national/27BOIS.html?ex=1084089284\&ei=1\&en=bd65293d3d6b1e62$ 

The U.S.A.P.A.T.R.I.O.T. (Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism) Act makes it a crime to provide "expert guidance or assistance" to groups deemed terrorist. As a result, 34year-old Sami Omar al-Hussayen of Saudi Arabia, a PhD candidate in computer science at the University of Idaho, was charged with three counts of conspiracy to support terrorism and 11 counts of visa and immigration fraud for being the Webmaster for several Islamic organizations, some of which had Web links to other sites where people praised suicide bombers in Chechnya and in Israel. He was charged with providing "computer advice and assistance, communications facilities, and financial instruments and services that assisted in the creation and maintenance of Internet Web sites and other Internet medium intended to recruit and raise funds for violent jihad, particularly in Palestine and Chechnya."

Defense lawyers denied that Mr. Hussayen sympathizes with extremist views; prosecutors claim that he is a secret terrorist. Civil liberties advocates argue that the law is so broad that "Somebody who fixes a fax machine that is owned by a group that may advocate terrorism could be liable," according to Prof. David Cole of the Georgetown University school of law. Judge Audrey B. Collins of the Federal District Court in Los Angeles wrote in another case dealing with the U.S.A.P.A.T.R.I.O.T. Act that "a woman who buys cookies at a bake sale outside her grocery store to support displaced Kurdish refugees to find new homes could be held liable" if the sale were sponsored by a group that were designated terrorist by the government.

Civil liberties activists also point out that the defendants activities as Webmaster and dealing entirely with ideas and statements are supposed to be protected by the First Amendment of the US Constitution.

Category 16.3	Infrastructure protection $\&$ homeland security
2004-04-27	Homeland Security NSA team up cybersecurity COAEIAE

DHS IAIP Daily;

http://fcw.com/fcw/articles/2004/0426/web- nsa- 04- 27- 04.asp

April 27, Federal Computer Week — DHS, NSA team on cybersecurity.

On April 22, officials from National Security Agency (NSA) and the Department of Homeland Security (DHS) announced the formation of the National Centers of Academic Excellence in Information Assurance Education. It stems from NSA's Centers of Academic Excellence in Information Assurance Education Program, which started in 1998 and recognizes 50 universities in 26 states. The National Strategy to Secure Cyberspace, issued in 2002 by the Bush administration, directs the government to foster training and education programs that support computer security needs and responsibilities, and improve existing information assurance programs. Earlier this month, NSA officials announced they would hire 1,500 people by September and 1,500 employees each year for the next five years. Agency jobs include information technology and acquisition positions in addition to traditional code- making and code- breaking roles, according to an April 7 statement.

Category 16.3 Infrastructure protection & homeland security

### 2004-04-28 PATRIOT act ACLU civil liberties constitution privacy terrorism anti-terrorism US government

NewsScan

[U.S.A.P.A.T.R.I.O.T.]... ACT RULES MUFFLE DISSENT

The secrecy provisions of the ...[U.S.A.P.A.T.R.I.O.T.] Act have prevented the American Civil Liberties Union from publicizing a lawsuit it filed three weeks ago challenging the FBI's methods of obtaining many business records. The ACLU was recently allowed to release a redacted version of the lawsuit following extended negotiations with the Justice Department. "It is remarkable that a gag provision in the Patriot Act kept the public in the dark about the mere fact that a constitutional challenge had been filed in court," says ACLU associate legal director Ann Beeson. "President Bush can talk about extending the life of the Patriot Act, but the ACLU is gagged from discussing details of our challenge to it." The crux of the ACLU's case concerns a section of the Act that allows the FBI to request financial records, telephone and e-mail logs, and other documents from businesses without a warrant or judicial approval. Such requests are known as "national security letters," and the FBI has issued scores of such letters since late 2001. The ACLU complaint says that using national security letters to force Internet service providers to turn over names, screen names, e-mail addresses and other customer information without proper notice to customers raises questions about the constitutionality of the ...[U.S.A.P.A.T.R.I.O.T.] Act's legal underpinnings. (Washington Post 29 Apr 2004)

### Category16.3Infrastructure protection & homeland security2004-05-03first responder communications network Homeland Security incident management

DHS IAIP Daily;

http://home.businesswire.com/portal/site/google/index.jsp?ndmViewId=news\_vie w&newsId=20040503005637&newsLang=en

May 03, Business Wire — Responder network to be installed in Kansas agencies.

A \$993,500 grant from the U.S. Department of Justice was awarded to the University of Kansas to install a Homeland One First Responder Network across the state of Kansas. The Kansas Law Enforcement Training Center and the Kansas Fire and Rescue Training Institute, both units of University of Kansas Continuing Education, will administer the grant. The grant calls for Homeland One First Responder Training and Communications Network to be installed at 319 Kansas law enforcement and fire services agencies across the state. "The University of Kansas has been a recognized leader in providing law enforcement and fire service training for more than 60 years," said JoAnn Smith, vice provost for university outreach and dean of Continuing Education at the University of Kansas. Homeland One's training modules are modeled on National Interagency Incident Management Systems and based on the Department of Homeland Security's Office for Domestic Preparedness (ODP) First Responder Training Guidelines and Standardized Emergency Management System (SEMS) standards.

Category 16.3 Infrastructure protection & homeland security

#### 2004-05-03 wireless federal government Homeland Security

DHS IAIP Daily;

http://www.fcw.com/fcw/articles/2004/0503/pol- wireless- 05- 03 - 04.asp

May 03, Federal Computer Week — Agencies team to develop integrated wireless network.

The Integrated Wireless Network (IWN) will provide a common wireless infrastructure to support the departments of Homeland Security, Justice, and Treasury, and officials expect to release their requirements this summer. Bringing three diverse departments together can be challenging, said Mike Duffy, Justice's deputy chief information officer for e- government, citing as an example the number of people needed to approve a memorandum of understanding. But the three agencies' leaders see the benefits and are committed to the project, he said. "The architecture analysis we conducted show there are substantial savings to be had both in cost and spectrum use by consolidating the three departments' resources," Duffy said. The new network will replace the aging wireless systems in many of the departments' components and will be designed to serve more than 80,000 law enforcement and homeland security users at 2,500 radio sites. The statement of objectives for IWN will be released in June or July and will outline the expectations and constraints of the project, officials said. Although the project will initially focus on voice capabilities, it will soon require wireless data capabilities, officials said. Also, the standards- based system must work with state and 10 local law enforcement systems.

Category 16.3 Infrastructure protection & homeland security

#### 2004-05-04 business continuity planning disaster recovery federal government

DHS IAIP Daily; http://www.gcn.com/23\_10/homeland- security/25793- 1.html

May 04, Government Computer News — Agencies take notice of continuity planning.

Next week, more than 2,500 federal employees from 45 agencies will test how prepared the government is to stay open if disaster strikes. The Homeland Security Department's Emergency Preparedness and Response Directorate, which still uses the acronym FEMA, will run Exercise Forward Challenge to see how far along agencies are in developing and implementing continuity of operations plans, or COOPs. During the exercise, employees will go to alternate work sites outside Washington and then try to hook up to their networks, access e- mail and data files, communicate with other federal officials and perform their usual tasks. "This is a full- scale operation designed to test interdependencies and essential functions," FEMA undersecretary Michael Brown said. "Agencies will find out if their plans 9 work, and it will give them a wake- up call to fix any problems." Brown last month told lawmakers he is confident that agencies are prepared. Linda Koontz, director for information management issues for the General Accounting Office, expressed less optimism. She told the committee that she would not guarantee that agencies would continue to operate at full capacity if a catastrophe hit the Washington area.

# Category 16.3 Infrastructure protection & homeland security 2004-05-04 Virginia Information Technologies Agencies VITA template business continuity planning

DHS IAIP Daily; http://www.gcn.com/23\_10/homeland- security/25813- 1.html

May 04, Government Computer News — Virginia uses software template to standardize its agencies' COOPs.

The Virginia Information Technologies Agency (VITA) is providing state and local government agencies with training and a template for establishing standard continuity of operations plans (COOPs). Paul Lubic, VITA's associate director for policy, practice and architecture, said his agency recently bought software to promote the adoption of best practices. "We see a value in using the template so the continuity of operations plans will be in a standard format, which will enhance the management of those plans at the governor's office level," Lubic said. "Having them all look the same will let us quickly navigate to get the information we need in case of an emergency." The software includes an online template that lets agencies create their plans and store them in a central repository. "To answer the questions, the agencies must have an understanding of their business and the processes that are critical to their mission," Lubic said. The system also can notify government workers in the event of a disaster via wireless e- mail devices.

### Category 16.3 Infrastructure protection & homeland security 2004-05-13 business continuity of operations planning coop federal government Homeland Security DHS

DHS IAIP Daily; http://www.dhs.gov/dhspublic/display?content=3554

May 13, Department of Homeland Security — Federal Government tests continuity of 8 operations plans.

The Department of Homeland Security (DHS) and more than 40 other agencies are testing their continuity of operations (COOP) plans during Forward Challenge 04 (FC 04), a two day exercise May 12- 13. The exercise is a full- scale, scenario- based event in which Federal departments and agencies are implementing COOP plans, deploying pre- designated personnel and leadership at alternate sites away from the National Capital Region and performing essential functions at those locations. In order to ensure Federal departments and agencies are prepared to continue essential operations during any type of threat or emergency, DHS maintains an active program of planning, testing, training and evaluation of the Federal Executive Branch COOP program. Forward Challenge 04 tests the federal government's readiness to respond and ability to resume critical operations during an emergency situation. "This is the first- time that the Federal government has conducted a government- wide test of its continuity of operations plans," said DHS Secretary Tom Ridge.

Category 16.3 Infrastructure protection & homeland security

2004-05-14 Homeland Security states Websites communication training events calendar

DHS IAIP Daily; http://www.govtech.net/news/news.php?id=90248

May 14, Government Technology — Oklahoma's redesigned Homeland Security Website.

Oklahoma's Office of Homeland Security recently launched an enhanced Website with several new interactive services that facilitate communication between the eight Oklahoma regional councils, its members and training officers. The Web site allows the public to see who is working on homeland security initiatives in their area while providing a secure electronic avenue for authorized users to communicate with officials and other select representatives. After successful login, authorized users can post messages and documents to regional bulletin boards. The training events calendar is accessible to the public and published on the Office of Homeland Security Web site. "The new Website is an excellent way for our office to communicate with the public and with responders, each of whom is essential to homeland security efforts," said Kerry Pettingill, director of the Oklahoma Office of Homeland Security.

2004-05-14	Homeland Security Data Analysis NVAC Federal Government
Category 16.3	Infrastructure protection & homeland security

DHS IAIP Daily;

http://fcw.com/fcw/articles/2004/0510/web- dhsvis- 05- 13- 04.as p

May 14, Federal Computer Week — DHS funds data center.

The Department of Homeland Security (DHS) has created a center to develop new methods and tools that would manage, analyze and graphically represent vast and diverse amounts of data to discover and predict potential terrorist activities. The Department of Energy's Pacific Northwest National Laboratory (PNNL), located in Richland, WA, will receive \$2.5 million this year for the new National Visual Analytics Center (NVAC) that will work on projects related to analyzing data that includes text, measurements, images and video. It's expected that NVAC will establish four or five regional visual analytics centers next year as funding becomes available. NVAC's core responsibilities include research and development, education, technology evaluation and implementation and integration and coordination of research programs across government agencies. It will not collect data but develop tools for new ways to evaluate information currently being used by counter- terrorism analysts. It will also work with university researchers to develop future visual analytics technology.

Category16.3Infrastructure protection & homeland security2004-05-17Homeland Security DHS SPIRIT, Resource Sharing

DHS IAIP Daily:

http://fcw.com/fcw/articles/2004/0517/news- dhs- 05- 17- 04.asp

May 17, Federal Computer Week — DHS regroups on SPIRIT; IT services pact delayed again.

The Department of Homeland Security (DHS) officials have decided to reassess their proposed five- year, \$5 billion information technology services program, delaying the release of the final request for proposals for at least another month. The Security, Planning and Integrated Resources for Information Technology (SPIRIT) program, which would cover nearly all IT services for DHS, was scheduled to be released this week. SPIRIT started as the Coast Guard Information Technology Services Solution in November 2002, but two months later officials decided it would be a departmentwide program valued at \$10 billion for 10 years. Since last summer, however, promises to release an RFP have failed to materialize at least six times.

#### Category 16.3 Infrastructure protection & homeland security

#### 2004-05-18 Homeland Security DHS customs data analysis

DHS IAIP Daily;

http://www.gcn.com/vol1\_no1/homeland- security/25913- 1.html

May 18, Government Computer News — Auditors warn of delays, overruns in Customs system.

The Department of Homeland Security's (DHS) massive new system for processing import- export data faces continuing cost and scheduling problems, the General Accounting Office (GAO) said on Tuesday, May 18. Customs and Border Protection, a DHS agency, last year inherited the Automated Commercial Environment project from the Customs Service. Since then, cost and scheduling problems have multiplied, GAO reported. ACE releases 1 and 2 cost \$109.4 million instead of the planned \$86.1 million, while releases 3 and 4 ballooned from \$146.4 million to \$192.4 million, GAO said. GAO said the customs agency coped by borrowing resources from forthcoming releases and overlapping activities to catch up with its schedule. Department officials said they agree with the auditors' conclusions and are working to correct the problems. The report is available at http://www.gao.gov/new.items/d04719.pdf

Category 16.3 Infrastructure protection & homeland security

#### 2004-05-18 trial internet terrorism Islamic Assembly North America Michigan

NewsScan

#### TRIAL OF MAN ACCUSED OF USING INTERNET FOR TERRORISM

In the terrorism trial of a University of Idaho computer science graduate student Sami Omar Al-Hussayen, a 34-year-old Saudi national, prosecutors say that they've proven a conspiracy between the defendant and the Michigan-based Islamic Assembly of North America to use the Internet to foster terrorism, and that they should therefore be allowed to show jurors Web postings about the Assembly that are not specifically related to Al-Hussayen. In rebuttal, Defense attorney David Nevin argues that his client is charged with promoting terrorism just because some Internet sites he helped maintain carried objectionable material: "We're circling around and around and making our way toward the issue of the First Amendment that has been floating around here from the start." Besides being accused of terrorist activities, Al-Hussayen is also accused of visa fraud and making false statements to cover up his association with the Assembly. (AP/USA Today 18 May 2004)

Category 16.3 Infrastructure protection & homeland security

#### 2004-05-19 security overreactions technology and society

DHS IAIP Daily;

http://www.fox11az.com/news/state/stories/KMSB- 20040519- famb p- bombscare.1d988929f.html

May 19, FOX11AZ (Tucson, AZ) — Bomb scare grounds America West plane.

An MP3 player wrapped around a soda can sparked a bomb scare at Phoenix Sky Harbor International Airport Wednesday morning, May 19, said an official with the Transportation Security Administration. Nearly 120 passengers on board the America West plane were evacuated Wednesday. The can was found in the cabin of America West Airlines flight 44 from Phoenix to Washington, DC. The bomb squad was called in and a bomb- sniffing dog was taken aboard the plane. All 117 passengers were safely evacuated. They will all be re- screened before they are allowed back on a plane to continue on to Washington. Investigators are looking into how the can came to be aboard the plane.

Category 16.3 Infrastructure protection & homeland security

2004-05-20 Homeland Security DHS overreaction subway photo video ban

DHS IAIP Daily; http://www.wnbc.com/traffic/3328661/detail.html

May 20, Associated Press — Possible ban on subway photos, videos to deter terrorists.

New York Transit officials on Thursday, May 20, proposed banning photography on subways and buses for their more than seven million daily riders to deter terrorists from conducting surveillance of the nation's largest mass transit system. NYC Transit, the division of the Metropolitan Transportation Authority that runs the subways, the buses and the Staten Island Railway, said the ban on photography and videotaping would not apply to journalists with valid ID cards or to people with written permission. Officials have paid increasing attention to transit security as the Republican National Convention approaches and following the March 11 Madrid commuter train bombings, which killed 191 people. NYC Transit President Lawrence Reuter said the rule changes were "intended to enhance security and safety" for customers and employees. NYC Transit also proposed banning passengers from using end doors to move from one subway car to another, putting feet up on seats and standing on skateboards on subways or buses, among other changes. Violators of the rules would be subject to fines. The changes need MTA board approval after a 45- day period of public comment.

Category 16.3	Infrastructure protection & homeland security
2004-05-24	monitor visitors inside United State U.S. Homeland Security Computer identification databases track systems

NewsScan

SYSTEM FOR TRACKING VISITORS TO U.S.

The Department of Homeland Security is getting ready to award a very large contract (perhaps worth as much as \$15 billion) for a network of databases to track visitors to the country before and after they arrive. The system will attempt to show where the visitors are going and whether they pose a terrorist threat. The three companies vying for the contract, which is called US-Visit, are Accenture, Computer Sciences, and Lockheed Martin. Visitors arriving at checkpoints will face real-time identification to confirm they are who they say they are and to make it possible to track them while they remain inside the U.S. Asa Hutchinson of Homeland Security says, "This is hugely important for the security of our country and for the wise use of our limited resources. We're talking here about a comprehensive approach to border security." Civil libertarians are alarmed that the databases could, despite assurances from the Homeland Security department, be used to monitor American citizens. (New York Times 24 May 2004)

Category	16.3	Infrastructure protection $\&$ homeland security
----------	------	--

2004-05-31 Homeland Security foreign visitor tracking surveillance Accenture

NewsScan

#### ACCENTURE BID WINS HOMELAND SECURITY PROJECT

The Department of Homeland Security has awarded Accenture LLP a contract worth up to \$10 billion to expand a program called "U.S. Visit" designed to track millions of foreign visitors from the time they arrive until the time they leave. The data collected by the system includes digital

photographs and fingerprints, and is used to help authorities capture suspected terrorists and criminals. Department of Homeland undersecretary Asa Hutchinson say, "I don't think you could overstate the impact of this responsibility, in terms of security of our nation. If you look at the 9/11

terrorists, they came here in violation of our immigration laws." The subcontractors in the Accenture team include AT&T, Dell, and KBR, and 26 others. (Washinton Post 2 Jun 2004)

#### Category 16.3 Infrastructure protection & homeland security

#### 2004-06-02 **border controls homeland security technology biometrics**

http://www.nytimes.com/2004/06/02/technology/02secure.html?th=&pagewante d=print&position=

Bermuda-based Accenture was awarded a multibilion-dollar contract by the Department of Homeland Security to establish high-technology border controls in a projected called "US-Visit." Critics complained that the contract should have gone to a firm that pays US taxes, but Accenture retorted that it does, and it has 25,000 employees in Reston, VA. The project will integrate dozens of federal databases and could use the biometric identification and authentication technologies to control traffic into the US.

Category 16.3	Infrastructure protection $\&$ homeland security	
---------------	--	--

#### 2004-06-16 Internet protocol IP voice over VoIP deregulation terrorism control fear

NewsScan

TERROR OVER INTERNET PROTOCOL?

A senior Justice Department official has told a Senate committee that law enforcement faces new threats from Internet-based telephone services, and warned that legislative efforts to deregulate VoIP (Voice over Internet Protocol) services could undermine the ability of law enforcement officials

to investigate criminal or terrorist activity. The Justice Department has asked the FCC to require Internet phone companies to design electronic conduits in their networks that would make it easier to tap conversations. James X. Dempsey of the Center for Democracy and Technology says that a

better approach would be for investigators to work cooperatively with Internet phone providers. (Washington Post 16 Jun 2004)

Category 16.3 Infrastructure protection & homeland security

#### 2004-07-16 al-Qaeda information files pictures Arkansas computer anti-terrorism Homeland Security incident

NewsScan

'ISOLATED INCIDENT': AL-QAEDA FILES ON ARKANSAS COMPUTER

A state computer in Arkansas has been found to contain texts and images that apparently originated with the terrorist group al-Qaeda, but Gary Underwood, chief security officer for the state computer network, says the terrorist-related files were an isolated incident. He received responses from 34 of the 80 agencies he e-mailed Wednesday and said: "The vast majority of those do not have FTP servers at all. Several others responded they had basically private, internal FTP servers used among staff and offices of the agency. Those are secure, user-name and password protected. There were a few that do have publicly accessible FTP servers, but all of those, including now the highway

department, do not allow anonymous uploads. They require a user identification or password to access... Obviously, what happened the other day raised everybody's awareness. If anybody had any questions, they immediately went to find out whether or not it was secure," (AP/USA Today 16 Jul 2004)

# Category 16.3 Infrastructure protection & homeland security 2004-07-19 anti-terrorism Homeland Security database Americal Civil Liberties Union ACLU privacy concerns

NewsScan

MATRIX RELOADED

The crime and terrorism database known as Matrix (the Multistate Anti-Terrorism Information Exchange) is being changed in response to various privacy and legal concerns -- yet not all of Matrix's critics are reassured by the changes. Some of the changes are intended to decentralize the database administration, but Barry Steinhardt of the American Civil Liberties Union says, "Decentralized data which is just as easily accessed as centralized data creates the same privacy problems." Matrix organizers say that the system is entirely limited to information they have always been able to obtain without a warrant. (San Jose Mercury News 19 Jul 2004)

Category 16.3	Infrastructure protection $\&$ homeland security
2004-07-20	underwater security summer 2004 Athens Olympic Games Greece fiber-optic network

NewsScan

UNDERWATER SECURITY IN ATHENS

As part of the preparations for the upcoming Olympic games in Athens, sea divers have installed an underwater monitoring network of fiber-optic cables wrapped in green plastic. Protesters contend the network is a privacy invasion. A police spokesman said: "The security measures are being

implemented with complete respect for human rights and according to the guidelines set out by the agency responsible for privacy and data protection" -- but a protest group called Campaign Anti-2004 complains: "For us the Olympic Games are not welcome. The culture of the Olympic Games is not out a " (AP (USA Today 20 kt) 2004)

not ours." (AP/USA Today 20 Jul 2004)

Category 16.3 Infrastructure protection & homeland security

2004-07-21 anti-terrorism software law enforcement Homeland Security TimeWall information analysis

NewsScan

2004-08-16

SOFTWARE FOR TRACKING TERRORISTS

TimeWall, 3-D virtual presentation developed by a Xerox spinoff called Inxight, tracks people, places, relationships and events, filtering huge amounts of unstructured information from a variety of sources (e.g., e-mail and Internet reports) in two dozen languages, and finding phone numbers, names and other data to identify relationships, patterns and trends. Inxight founder and chief technology officer Ramana Rao explains: "Rather than an intelligence analyst reading all this stuff to decide what is interesting, the software pulls it out automatically and puts it on the wall." The software searches through information in real time and sorts data into various bands, arranged chronologically. The analyst can then move along the bands to go backward or forward in time to see how relationships or events change. (San Jose Mercury News 21 Jul 2004).

Category 16.3 Infrastructure protection & homeland security

### Internet terrorism information Web scanner detection 95% text based pattern recognition terror content hits surfers

DHS IAIP Daily; http://www.haaretz.com/hasen/spages/465047.html

August 16, Haaretz (Israel) — Web scanner can detect terror content.

Engineering faculty researchers at Ben- Gurion University (BGU) in Israel reported Sunday, August 15, that they have developed a system that can identify 95 percent of Internet pages with terrorism- related content. The experimental system, which is being developed to detect information regarding terror activity automatically, was designed by Dr. Mark Last of the Department of Systems Information Engineering at BGU, and Prof. Abraham Kandel of the National Institute for Systems Test and Productivity, in the United States. The system is based on the recognition of patterns in texts with terror content, based on examples from existing Internet sites. It uses these patterns to identify "hits" by surfers on other sites with similar characteristics, in order to locate users affiliated with terror organizations and new sites set up by terrorist elements, among other things. According to Last, the development has great importance in view of the considerable use of the Internet in coordinating and orchestrating terror acts. "The lack of ability to enforce limitations on Internet users allows terror organizations to set up Internet sites that spread incitement, raise money in support of terror and find new supporters for their causes," Last said.

## Category16.3Infrastructure protection & homeland security2004-08-16cyberterrorism training Homeland Security Arkansas Center Little Rock critical<br/>infrastructure protection

DHS IAIP Daily;

http://www.usatoday.com/tech/news/2004- 08- 16- cyberterror- gra nts- ark\_x.htm

August 16, Associated Press — Arkansas center to train officers in cyberterrorism.

Department of Homeland Security Undersecretary Asa Hutchinson announced on Sunday, August 15, a \$34 million grant program that will be shared among 14 groups nationwide to counter terrorism. The National Center for Rural Law Enforcement in Little Rock was among the 14 groups that will share in the training grant program. The center is part of the University of Arkansas' Criminal Justice Institute, and was awarded \$2.8 million of the total grant to train rural law enforcement officers to recognize cyberterrorism, preserve the physical evidence as they would any crime scene, and notify the appropriate federal agency. Hutchinson said said cyberterrorism presents a threat to the country's security and the operation of utilities, government infrastructure, and commerce. A majority of the nation's power companies report some kind of "cyber attack" at least once a year, he said. The program out of the Little Rock center will address such cybercrime as computer hacking into sensitive files, computer viruses, and the breakdown in water and sewer systems because of a computer adjustment to the controls, he said.

Category	16.3	Infrastructure protection & homeland security
2004-08-1	6	Department Homeland Security Microsoft Windows XP service pack 2 SP2 testing US-CERT

DHS IAIP Daily;

http://www.fcw.com/fcw/articles/2004/0816/news- dhs- 08- 16- 04. asp

August 16, Federal Computer Week — DHS recommends agencies test Windows SP2.

The Department of Homeland Security's U.S.- Computer Emergency Readiness Team (US- CERT) is recommending that all Microsoft Windows XP users, including agencies, carefully test the company's newest security patch, Service Pack 2, and then deploy it throughout their organizations. US- CERT officials view the patch as a step in the right direction because it "makes Internet Explorer highly resistant to the types of attacks we've seen recently, such as download.ject, and enables Windows firewalls." Download.ject is a Trojan horse program 10 that attempts to download and install a file by exploiting vulnerabilities in Microsoft's Internet Explorer Web browser. Testing is important. Security features embedded in the upgraded operating system will be turned on by default, for example, and because users are being urged to install SP2 through automatic download, people unfamiliar with security policies could suddenly be faced with having to make vital decisions about their systems' protection. Those default features also could break certain custom applications that agencies have developed.

Category 16.3 Infrastructure protection & homeland security

#### 2004-08-19 National Institute of Standards and Technology NIST security configuration checklist Windows 2000 2K XP Homeland Security sponsor

DHS IAIP Daily;

http://fcw.com/fcw/articles/2004/0816/web- nist- 08- 19- 04.asp

August 19, Federal Computer Week — NIST makes lists.

Officials at the National Institute of Standards and Technology (NIST) recently announced that a security configuration checklists program for information technology products, including a logo that vendors can put on their wares, is on track for completion before the end of 2004. A security configuration checklist describes the software options and settings that users can choose to minimize the security risks associated with a particular type of hardware or software. NIST officials will distribute the lists through a Web portal, checklists.nist.gov. NIST officials have already published two security checklists, one for Microsoft Corp.'s Windows 2000 and XP Professional: csrc.nist.gov/itsec. NIST's authority for creating the security checklist program comes from a 2002 law, the Cyber Security Research and Development Act. The Department of Homeland Security is listed on NIST's Website as a program sponsor.

## Category 16.3 Infrastructure protection & homeland security 2004-08-27 US ISPs companies terrorist information Website hosting partnership freedom of speech contractual agreement

DHS IAIP Daily;

http://www.cnsnews.com/ViewForeignBureaus.asp?Page=%5CForeig nBureaus%5Carchive%5C200408%5CFOR20040827d.html

August 27, Cybercast News Service — U.S. companies providing indirect service to terrorist websites, report says.

American Internet Service Providers are being used indirectly by the Palestinian Islamic Jihad and other terrorist groups to market their terrorist messages, Israel's Intelligence and Terrorism Information Center at the Center for Special Studies said in a recent report. "Palestinian and international terrorist organizations make massive use of the Internet to spread propaganda supporting terrorism and as a means of maintaining contact between organizations and headquarters, their infrastructures and their target populations," the report said. Two of the companies listed in the report said they were now in the process of correcting the situation. Preference for U.S. and Western companies provides terror groups with "advanced technological support," the ability to "disappear" among the multitudes of Western companies on the Internet - - and to a certain extent, allows protection under U.S. freedom of speech guarantees, the report adds. Brian Marcus, director of Internet monitoring for the Anti- Defamation League in New York, said that laws governing the posting of terrorism- related material on websites fall into a "gray area," but service agreements may enable companies to close down websites. Report: http://www.intelligence.org.il/eng/sib/8\_04/internet.htm

Category 16.3 Infrastructure protection & homeland security

2004-08-30 US states cyberattack alert plan risk assessment color code network security threats Homeland Security

DHS IAIP Daily; http://www.nwfusion.com/news/2004/083004nastd.html

August 30, Network World — States prepping cyberalert plan.

Looking to gauge the risk of attacks against their networks, state officials this week will vote on new measures that would assess threats and dictate specific actions to take to protect key resources. If adopted, the common alert- level procedures would color- code the threat to state networks and recommend action to take in response to specific threats. The proposed cybersecurity alert system would establish a secure Website state officials could tap to determine why each state has the security ranking it does and whether they should take action based on what other states experience. Homeland security ranked among the key topics considered last week at the National Association of State Telecommunications Directors (NASTD).

Category 16.3 Infrastructure protection & homeland security

2004-08-30 New York City information technology IT disaster recovery plan

DHS IAIP Daily; http://www.eweek.com/article2/0,1759,1640674,00.asp

August 30, eWEEK — NY IT prepares for disaster recovery.

As New York City braces for the Republican National Convention (RNC) this week, IT managers at the city's financial services companies may be nervous about the potential for terrorism, but they're prepared. Having learned from the terrorist attacks of September 11, 2001, and the massive power blackout of 2003, many Manhattan- based companies are now hardened with beefed- up disaster recovery initiatives, such as encrypted data backup processes, remote backup facilities and redundant telecommunications systems. While the threat of terrorism has remained somewhat of a constant in New York, the RNC has pushed companies located in the area around Madison Square Garden to aggressively plug any holes in their disaster recovery strategies. The RNC's IT staff said they are ensuring that their own systems remain open at all times. "Our first line of defense is redundancy. Most everyone has a cell and a land line," said Max Everett, director of IT for the RNC. "We're working directly with the Secret Service and US- CERT to ensure our data integrity and network security."

## Category 16.3 Infrastructure protection & homeland security 2004-09-01 terrorism antiterrorism Homeland Security Al Qaeda technology computers critical infrastructure protection arrests

DHS IAIP Daily; http://www.pcworld.com/news/article/0,aid,117658,00.asp

September 01, PC World — Al Qaeda's tech traps.

Al Qaeda and other terrorist groups are becoming more technically adept at using the Web and computers. The arrest of alleged Pakistani terrorist Mohammad Naeem Noor Khan, captured this summer with 51 optical discs and three computers full of terror intelligence, is the most recent indicator. For the past ten years, dissidents from the Middle East, Chechnya, and Latin America have used the Internet to further their cause, says Josh Devon, a senior analyst at the SITE Institute, a terrorism research group that monitors the Web. But the proliferation of the Web and the availability of more powerful and affordable graphics and multimedia processing tools have dramatically increased al Qaeda's and other terrorist groups ability to communicate, to broadcast their message, to create public lists of who and what to target, and to train others much more than was possible even five years ago. While technology can make it easier to conceal information and communicate covertly using digital tools such as encryption, it also leaves digital trails of evidence. Computer intelligence found on Khan's computers was instrumental in the arrests of Pakistani and UK terror suspects.

## Category 16.3 Infrastructure protection & homeland security 2004-09-01 information security technology human factors terrorism Homeland Security linguistics computation Arabic language

DHS IAIP Daily; http://www.gcn.com/vol1\_no1/daily- updates/27131- 1.html

September 01, Government Computer News — The human factor trumps IT in the war on terror.

Computer scientists at the University of Maryland are pushing the technology envelope to assist in intelligence gathering and analysis, but the people using the data may be the limiting factor in its effectiveness. "While there is a lot of good information out there, it isn't getting to the right people at the right time," said William J. Lahneman, coordinator of the Center for International and Security Studies in the School of Public Policy. Implementing recent presidential directives on moving data across agency lines will require not only changing IT architectures, but will "challenge the very culture" of those agencies, said James Hendler of the university's Institute for Advanced Computer Studies. Hendler is focusing on the intelligence needed to use the Web effectively in gathering information and answering questions. The university's Computational Linguistics and Information Processing Lab is developing more- fluent automated translation systems for languages such as Arabic. Co- director Amy Weinberg said the lab also is working on how to rapidly ramp up systems to handle new languages as new threats develop. Some terrorist groups already are ahead of the government in their use of existing Web technology to win the hearts and minds of people, said Lee Strickland, director of the university's Center for Information Policy.

## Category 16.3 Infrastructure protection & homeland security 2004-09-02 US government agencies software security quality assurance Homeland Security DHS IA Directorate

DHS IAIP Daily; http://www.infoworld.com/article/04/09/02/HNusgovt\_1.html

September 02, IDG News Service — U.S. government agencies aim for software assurance.

U.S. government agencies need to better understand the vulnerabilities of the software they're buying, said IT workers from several government agencies during a software assurance forum in Washington, D.C., last week. The forum, sponsored by the Department of Defense (DoD) and the Department of Homeland Security (DHS), was the first step in a long- term discussion between government agencies and vendors on how to create more secure software, said Joe Jarzombek, deputy director for software assurance in the DoD Information Assurance Directorate. Prompting the forum was "a growing awareness of the fact that we've got a lot of vulnerabilities in the software we're acquiring," said Jarzombek. A major concern among government IT workers is a need to understand how and where software is developed. In many cases, software used by government agencies is developed by outsourced workers, Jarzombek said, and government purchasers need to know that information. Software developers should expect more security demands from customers in the near future, added Mike Rasmussen, principal analyst Forrester Research Inc. Government agencies are under pressure from Congress to improve their cybersecurity, and agencies are moving toward making more security demands of software vendors.

Category16.3Infrastructure protection & homeland security2004-09-17Department Homeland Security DHS cyber security industry

DHS IAIP Daily; http://www.eweek.com/article2/0,1759,1647410,00.asp

September 17, eWeek — DHS follows industry lead on cyber- terror.

Lawrence Hale, deputy director of the Department of Homeland Security's (DHS) cyber security division, said Friday, September 17, that the DHS depends on the private sector to take the lead in fighting cyber- terrorist threats. "The normal things you do to protect your network will help protect you against cyber- terrorism," he said. Speaking at a conference on cyber- security organized by NBC News and the Northern Virginia Technology Council, Hale said the department is already aware of some cyber- terror threats, as well as the activities of terrorist organizations on the Internet. "They're using cyberspace for recruiting, fund- raising and communication," he said. Private- sector businesses in the United States are already taking the lead in making sure that they are protected against attacks and intrusion, according to Hale - - and the government is following their lead. While he wouldn't divulge details, Hale said the government is working to lessen the severity of any attack on it. He said the fact that most federal departments and agencies design and build their own networks and computer systems makes it less likely that any one type of attack would succeed across the government. He also explained that the department wants to expand its role with private businesses in its fight against cyber terrorism.

 Category 16.3
 Infrastructure protection & homeland security

 2004-09-19
 cyberterrorism information Internet Website identification algorithm Ben-Gurion University BGU

DHS IAIP Daily; http://www.jpost.com/servlet/Satellite?pagename=JPost/JPArticle/ShowFull&cid=1095565998846

September 19, Jerusalum Post (Israel) — Algorithms can identify cyber- terrorism.

Professor Mark Last of the Ben- Gurion University (BGU) department of information systems engineering is working on ways to make terrorist's communication on the Internet more difficult by conducting pioneering research on fighting terror in cyberspace. "The Internet helps terrorists a great deal, and makes their life easier in many senses - - because it is really a very difficult problem to find something suspicious in the sea of traffic. Access to the Internet is relatively easy and affordable worldwide, and it is easy to use while concealing your identity," Professor Last says. His team has developed an experimental system that succeeded in identifying about 95% of Web pages with a terrorist content. Last's cooperation with colleagues at the University of South Florida led to the U.S. National Institute of Systems Test and Productivity in Florida getting involved in the subject. His lab is now working as a subcontractor for the National Institute to design methods that will enable government agencies and commercial companies to improve security, quality and cost effectiveness of large- scale information systems, with a focus on cyber- terror. Their ability to distinguish cyber- terror activity from normal activity is becoming increasingly more reliable thanks to changes in the algorithms.

Category 16.3 Infrastructure protection & homeland security

#### 2004-10-01 US Department Homeland Security cybersecurity chief Amit Yoran resignation

DHS IAIP Daily;

http://www.washingtonpost.com/wp- dyn/articles/A64915- 2004Oct 1.html

October 01, Associated Press — U.S. cybersecurity chief resigns.

The government's cybersecurity chief has abruptly resigned after one year with the Department of Homeland Security. Amit Yoran informed the White House about his plans to quit as director of the National Cyber Security Division and made his resignation effective at the end of Thursday, September 30. Yoran said he "felt the timing was right to pursue other opportunities." It was unclear immediately who might succeed him even temporarily. Yoran's deputy is Donald "Andy" Purdy, a former senior adviser to the White House on cybersecurity issues.

Category 16.3 Infrastructure protection & homeland security

2004-10-05 critical infrastructure protection control systems vulnerable report hackers viruses

DHS IAIP Daily;

http://www.forbes.com/business/feeds/ap/2004/10/05/ap1577435.html

October 05, Associated Press — Experts say control systems vulnerable. Businesses and government agencies must re- examine the growing threat of cyberterrorism to automated computer systems running power grids, dams and other industrial facilities, security experts said at a conference Tuesday, October 5. From 1982 until about 2000, problems with such systems usually were associated with internal accidents or inappropriate employee behavior, said Eric Byres, manager of Critical Infrastructure Security Research at the British Columbia Institute of Technology. But a review by Byres of the last three years showed that 90 percent of these problems come from break- ins by hackers and computer viruses.

### Category16.3Infrastructure protection & homeland security2004-10-07schools terrorism data loss information warfare surveillance threat Iraq

NewsScan; http://www.usatoday.com/tech/news/2004-10-07-school-disk x.htm

TERROR IN THE INFORMATION AGE

Law enforcement authorities have notified school districts in six states that a computer disc found by the U.S. military in Iraq contained photos, floor plans and other information about their schools. The officials say there is no evidence of any specific plans to stage Beslan-like terrorist attacks on the schools, which are in Georgia, Florida, Michigan, New Jersey, Oregon and California. Schools have been urged to watch for various activities which, though legitimate on their own, which may suggest a threat if many of them occur together: interest in obtaining site plans for schools, bus routes and attendance lists; prolonged "static surveillance" by people disguised as panhandlers, shoe shiners, newspaper or flower vendors or street sweepers not previously seen in the area; observation of security drills; and so forth. Clevelandbased school safety consultant Kenneth Trump says: "It's a positive sign that they're finally discussing this after years of downplaying or denying even the possibility of a terrorist strike on schools. Public officials are in fear of creating fear, but we have to put the cards on the table, educate people in the school community and make sure they are well prepared."

Category 16.3	Infrastructure protection & homeland security
2004-10-08	Municipal Websites information terrorism clues weakness disclosure

DHS IAIP Daily;

http://washingtontimes.com/metro/20041007-113112-4486r.htm

October 08, Washington Times — Municipal Websites may help terrorists plot attacks.

Too many details on municipal Websites can tip off terrorists to security weaknesses and vulnerable targets, a military researcher told a conference of U.S. mayors in Washington, D.C. on Thursday, October 7. Gerald G. Brown, distinguished professor of operations research at the Naval Postgraduate School in Monterey, CA, said municipal leaders must not confuse "sunshine" laws, which require public access to some government data, and the allure of "really cool Websites." Brown said that seemingly innocuous information, such as budget data, can become fodder for terrorist plots. "Frequently these sites are used to ask for things: 'We need a firetruck. We need a Hazmat crew,' " Brown said. "If I'm attacking you, that's pretty good information."

#### Category 16.3 Infrastructure protection & homeland security

### 2004-10-10Terrorism Knowledge Base terrorist information collection FBI CIA Rand<br/>Corporation Department Homeland Security funding

DHS IAIP Daily;

http://www.chicagotribune.com/technology/chi- 0410100381oct10 ,1,6912082.story?coll=chi- techtopheds- hed

October 10, Chicago Tribune (IL) — Site tracks and charts terrorism information.

The Terrorism Knowledge Base, an online database available at http://www.tkb.org includes detailed reports on more than 18,000 terrorist incidents and nearly 1,000 terrorist groups and their leaders dating back to 1968. The database is still in its final shakedown stage, but it is already available for public use. Created by the National Memorial Institute for the Prevention of Terrorism in Oklahoma City, the database represents the largest repository of international terrorism information ever made publicly available on the Internet. Information sources include the FBI, the CIA and the Rand Corporation, a non- profit research think tank that for the first time is making its proprietary terrorism incident database- - long regarded by government experts and scholars as the world's most extensive- - available to the public. The Department of Homeland Security is providing some of the funding to support the project. The intended audience ranges from citizens curious about terrorism to journalists, researchers, intelligence and law- enforcement agencies, and even spies in the field working clandestine assignments.

# Category 16.3 Infrastructure protection & homeland security 2004-10-11 chat-room instant messaging IM surveillance anti-terrorism RPI professor Bulent Yener chatter pattern recognition algorithm National Science Foundation NSF grant

DHS IAIP Daily;

http://www.washingtonpost.com/wp- dyn/articles/A25272- 2004Oct 11.html

October 11, Associated Press — U.S. funds chat- room surveillance study.

The U.S. government is funding a yearlong study on chat room surveillance under an anti- terrorism program. A Rensselaer Polytechnic Institute computer science professor hopes to develop mathematical models that can uncover structure within the scattershot traffic of online public forums. Professor Bulent Yener will use mathematical models in search of patterns in the chatter. Downloading data from selected chat rooms, Yener will track the times that messages were sent, creating a statistical profile of the traffic. "For us, the challenge is to be able to determine, without reading the messages, who is talking to whom," Yener said. The \$157,673 grant comes from the National Science Foundation's Approaches to Combat Terrorism program. It was selected in coordination with the nation's intelligence agencies.

Category 16.3 Infrastructure protection & homeland security

#### 2004-10-14 state local homeland security IT program need federal guidance

DHS IAIP Daily; http://www.gcn.com/vol1\_no1/daily- updates/27632- 1.html

October 14, Government Computer News — CIOs: State and local homeland security IT needs more federal guidance.

State and local homeland security IT programs would be more effective if the federal government provided firmer standards and practices, senior federal officials said Thursday, October 14. Department of Homeland Security (DHS) CIO Steve Cooper, Justice Department CIO Vance Hitch and other high- level officials who spoke at an Industry Advisory Council meeting in Washington, D.C. agreed on the point. Cooper said he and Hitch should provide additional leadership to state and local governments on technology issues. Cooper noted that he was not necessarily talking about specific industry standards, but "the technology directions and the policies." DHS' state and local office has a weekly videoconference with state and local advisors, but that information may not reach all 89,000 municipalities, Cooper said.

Category 16.3 Infrastructure protection & homeland security

2004-10-15 Canadian anti-terrorism cyberterrorism force NSA Communications Security Establishment CSE

DHS IAIP Daily;

http://www.ctv.ca/servlet/ArticleNews/story/CTVNews/10978782 08404\_93287408/?hub=SciTech

October 15, Canadian Press (Ottawa) — Canada creates new force to fight cyber- terrorism.

A high- level national task force is being assembled to help Canada steel its defenses against potential cyber- attacks by terrorists. The head of Canada's electronic spy agency said the panel of private- and public- sector officials will help the country catch up to the United States in securing cyberspace. Communications Security Establishment (CSE) chief Keith Coulter noted Washington has already begun moving to protect their own key grids and networks. CSE, perhaps Canada's most secretive agency, has the dual role of helping protect crucial information- technology systems and eavesdropping on foreign communications. CSE and agencies in the United States, Britain, Australia and New Zealand share intercepted communications of interest with one another. Of particular importance is CSE's relationship with its American counterpart, the National Security Agency (NSA), Coulter said. "CSE and NSA share intelligence, tackle common problems posed by changing technology and track threats to our collective security."

#### Category 16.3 Infrastructure protection & homeland security

#### 2004-10-19 information security federal networks meeting DHS standards report

DHS IAIP Daily; http://www.gao.gov/cgi- bin/getrpt?GAO- 04- 375

October 19, Government Accountability Office — GAO- 04- 375: Information Technology: Major Federal Networks That Support Homeland Security Functions (Report).

A key information systems challenge in homeland security is ensuring that essential information is shared in a timely and secure manner among disparate parties in federal, state, and local governments, and in the private sectors. This requires communications networks that provide information- sharing capabilities between the various levels of government—federal, state, and local. The Government Accountability Office's (GAO) objective was to identify and describe, through agency reporting, major networks and examples of applications that the agencies considered important in supporting their homeland security functions. Nine agencies identified 34 major networks that support homeland security functions - 32 that are operational and two that are being developed. Of these 34, 21 are single- agency networks designed for internal agency communications. Six of the 34 are used to share information with state and local governments; four share information with the private sector. Highlights: http://www.gao.gov/highlights/d04375high.pdf

# Category 16.3 Infrastructure protection & homeland security 2004-10-27 database forged identities art cross border Rules of Crime Homeland Security DHS concern

DHS IAIP Daily;

http://www.nytimes.com/2004/10/27/arts/design/27iden.html?or ef=login

October 27, New York Times — How to cross borders, social or otherwise.

Heath Bunting and Kayle Brandon, two British artists, are compiling a database exploring elements of legal status in Britain, with the ultimate goal of allowing people to create a new identity from information collected on the Internet. The first stage of their project is the focus of "Rules of Crime," a show that runs through November 13 at the New Museum of Contemporary Art's temporary home in Chelsea, NY. In its final form, their project may be viewed as the Homeland Security Department's worst nightmare: a road map enabling all sorts of undesirables to penetrate a nation's borders, banking systems, supermarket loyalty clubs. Bunting and Brandon are among a growing number of artists who are harnessing technologies associated with governments and corporations to challenge the status quo. The Website for their project, known as the Status Project (http://status.irational.org) says it will eventually provide a how- to guide to getting a passport. The Status Project grew out of BorderXing, in which the artists documented illegal treks they made across European borders. The BorderXing Website, available for individual use by request (http://irational.org/cgi- bin/border/clients/deny.pl) offers pictures, suggested routes and tips for evading the authorities.

# Category 16.3 Infrastructure protection & homeland security 2004-10-27 Department Homeland Security DHS German Interior Ministry multilateral conference cyber security watch warning incident response

DHS IAIP Daily; http://www.dhs.gov/dhspublic/display?content=4077

October 27, Department of Homeland Security — Homeland Security and German Interior Ministry co- host multilateral conference on cyber security.

The U.S. Department of Homeland Security's Information Analysis and Infrastructure Protection (IAIP) Directorate and the German Ministry of the Interior co- hosted a multilateral conference in Berlin October 20- 22, 2004, on International Cyber Security Cooperation: Watch, Warning, and Incident Response. The conference consisted of delegations from fifteen countries including those from Europe, Asia Pacific and the Americas and represented a significant collaborative effort on the need for an international framework for cyber information sharing and incident response. The goal of the conference was to bring together government cyber security policy makers, managers of Computer Security Incident Response Teams (CSIRTs) with national responsibility, and members of the cyber law enforcement community. During the conference the participating countries discussed critical areas essential for building an international framework for cyber security, including: an arrangement among sovereign states to exchange cyber information, the incorporation of existing and emerging regional information sharing arrangements, and ways to improve information sharing in the near term and in the future.

## Category 16.3 Infrastructure protection & homeland security 2004-10-28 do not fly list airport TSA Transportation Safety Authority Kabay DNFL false positives authentication correction failure homeland security terrorism

NewsScan; Ubiquity

DO-NOT-FLY LISTS: DO-NOT-TAKE-SERIOUSLY!

The current issue of Ubiquity, an online publication of the ACM (edited by the editors of NewsScan), contains an article by Norwich University professor M.E. Kabay arguing that "the current implementation of do-not-fly lists and the use of documents to authenticate passenger identity won't necessarily improve airport security." A sample: "Deirdre McNamer (how appropriate) wrote a story in The New Yorker magazine in October 2002 about a 28-year-old pinko-gray-skinned, blue-eyed, red-blond-haired criminal called Christian Michael Longo who used the alias 'John Thomas Christopher.' His alias was placed on the DNFL used by the Transportation Security Administration. He was arrested in January 2002 but his alias was not removed from the DNFL. On March 23, 2002, 70-year-old brown-skinned, dark-eyed, gray-haired grandmother Johnnie Thomas was informed that she was on the master terrorist list and would have special security measures applied every time she flew. Indeed, the poor lady found that she was repeatedly delayed by a scurry of activity when she presented her tickets at an airline counter, extra X-rays of her checked baggage, supplementary examination of her hand-baggage and extra wanding at the entrance gates. On one occasion she was told that she had graduated to the exalted status labeled, 'Not allowed to fly.' She discovered that there was no method available for having 'her' name removed from the DNFL; indeed, one person from her local FBI office dismissively told her to hire a lawyer (although ironically, he refused to identify himself). An employee of the TSA informed her that 'four other law-abiding John Thomases had called to complain.'" (Ubiquity 28 Oct 2004)

Category16.3Infrastructure protection & homeland security2004-11-02computer data terrorism information extensible markup language XML metadata<br/>standard Homeland Security DHS FBI DoJ

DHS IAIP Daily;

http://www.fcw.com/fcw/articles/2004/1101/web- terrorxml- 11- 0 2- 04.asp

November 02, Federal Computer Week — Standardizing terror data.

Government officials crafting proposals for cross- agency counterterrorism information sharing plan to assign stewardship over a core set of Extensible Markup Language (XML) standards. Members of the Information Systems Council will identify XML standards and people responsible for them, said Bill Dawson, intelligence community deputy chief information officer at the CIA. Final plans are due to the president by December 24. Metadata standards enabling the widest possible dissemination of intelligence information are required under Section 3 of Executive Order 13356. On September 20, officials connected four previously incompatible systems - the FBI's Law Enforcement Online network, the Justice Department's Regional Information Sharing System, the Homeland Security Network and a criminal intelligence network in California.

Category 16.3 Infrastructure protection & homeland security

#### 2004-11-04 cybercrime hacker hiring FBI crime list 10 Best Wanted

DHS IAIP Daily;

http://www.washingtonpost.com/wp- dyn/articles/A25579- 2004Nov 4.html

November 04, Washington Post — More cyber- crime cases added to FBI list.

A former technology company executive charged with hiring hackers to attack a competitor's Website has joined the FBI's most- wanted list, the latest sign of the federal law enforcement agency's growing interest in cyber- crime. The most- wanted list is a group of more than a dozen people that includes some of America's most elusive criminals. It includes alleged embezzlers, an accused child pornographer and individuals indicted on drug and murder charges. The most- wanted list is not the same list as the notorious "10 Most Wanted," rather it is a list that the bureau started almost five years ago on its Website to nab suspects who are less of a threat or less prone toward physical violence, said spokesperson Paul Bresson. "This is the first time we've had such a significant number of people being investigated and prosecuted for computer crime," said Mark Rasch, a former prosecutor in the Justice Department's computer crimes and intellectual property section. "And we're only going to see this trend continue because investigators are getting better at identifying these individuals," said Rasch. The list, which currently includes 16 suspects, is located at http://www.fbi.gov/mostwant/alert/alert.htm

# Category 16.3 Infrastructure protection & homeland security 2004-11-08 counter terrorism data sharing extensible markup language XML Department Homeland Security DHS

DHS IAIP Daily; http://www.gcn.com/vol1\_no1/daily- updates/27854- 1.html

November 08, Government Computer News — Counterterror data sharing will rely on XML.

The Department of Homeland Security (DHS) will tweak the new Data Reference Model (DRM) to create a data model for the exchange of counterterrorism data. Under Executive Order 13356, DHS data architect Michael Daconta is leading a revision of the Federal Enterprise Architecture's 30- page DRM to share counterterrorism data while preserving individual privacy. At a meeting of the Association for Information and Image Management's National Capital Chapter in Arlington, VA, last week, Daconta said he is looking seriously at the way the Global Justice XML data model would handle metadata about agencies' watch lists. "XML is neutral" on concepts such as watch lists' heterogeneous collections, Daconta said, but it can bridge documents and data because its primary job is information exchange. Use of federated queries will require a standard governmentwide identifier for persons of interest, as well as a central registry for the metadata, Daconta said.

# Category 16.3 Infrastructure protection & homeland security 2004-11-30 Department Homeland Security DHS computer data network progress advance testing and accreditation SIPRNET

DHS IAIP Daily; http://www.informationweek.com/story/showArticle.jhtml;jsess ionid=XC2WBO3X2RJCIQSNDBCCKH0CJUMEKJVN?articleID=54201030

November 30, InformationWeek — Homeland Security Network advances.

The Homeland Security Department is moving forward with its plans to create a data network accessible to intelligence analysts and law enforcement across federal, state, and local boundaries. Homeland Security is moving into the testing and accreditation phase of its Homeland Secure Data Network, first introduced in April. The secure network, which could cost up to \$350 million to create, will initially connect Homeland Security intelligence personnel with the Defense Department's Secret Internet Protocol Router Network (SIPRNET) to send and receive information with classified security levels. Initiatives also are under way to next year connect Homeland Security, the Defense Department, and areas within the FBI and the greater intelligence community, including the CIA.

Category 16.3	Infrastructure protection & homeland security
	CIA Central Intelligence Agency Tenet cybersecurity concerns worries issues vulnerabilities homeland security terrorism

NewsScan;

http://www.washingtontimes.com/functions/print.php?StoryID=20041201-114750-6381r

EX-CIA CHIEF WORRIES ABOUT INTERNET SECURITY

Former CIA Director George J. Tenet sees the Internet as "a potential Achilles' heel" in the fight against terrorism, endangering "our financial stability and physical security if the networks we are creating are not protected." Calling for new cybersecurity measures, Tenet says: "I know that these actions will be controversial in this age when we still think the Internet is a free and open society with no control or accountability, but ultimately the Wild West must give way to governance and control." He believes that access to the Web might need to be limited to those who can show they take security seriously. (UPI/Washington Times 3 Dec 2004)

### Category16.3Infrastructure protection & homeland security2004-12-06committee cybersecurity post Department of Homeland Security DHS<br/>recommendation

DHS IAIP Daily;

http://www.fcw.com/fcw/articles/2004/1206/web- dhs- 12- 06- 04.a sp

December 06, Federal Computer Week — Committee pushes for cybersecurity post.

Members of the House Select Homeland Security Committee have recommended establishing a new assistant secretary position within the Homeland Security Department (DHS) to better integrate and coordinate cybersecurity issues. The recommendation is one of six suggestions listed in a new 41- page, bipartisan report that was released today by the committee's cybersecurity subcommittee. The report stated that although DHS officials have created the National Cyber Security Division and several other coordination entities, "now is the time to build toward more robust capabilities." It also stated DHS officials need to exert more effort to work with the private sector and across critical infrastructure sectors in addition to state and local governments. Report: http://hsc.house.gov/files/cybersecurityreport12.06.04.pdf

# Category16.3Infrastructure protection & homeland security2004-12-07cybersecurity serious attention computer security firms report CSIA research and<br/>development R&D Department Homeland Security DHS

DHS IAIP Daily;

http://news.com.com/Cybersecurity+post+needs+a+promotion%2C+ firms+say/2100-7348\_3-5481497.html

December 07, CNET News — Cybersecurity post needs a promotion, firms say.

The U.S. government is not taking cybersecurity seriously enough and should spend more money and energy on the topic, a group of computer security firms said Tuesday, December 7. At an event in Washington, DC, members of the Cyber Security Industry Alliance (CSIA) warned of the potential dangers of Internet attacks and called on the next Bush administration to create a new assistant secretary position inside the Department of Homeland Security, ratify the Council of Europe's cybercrime treaty, create an emergency coordination network to handle Internet outages, increase R&D funding for cybersecurity, and designate a federal agency to track the costs of cyberattacks. CSIA members include Check Point Software Technologies, McAfee, Symantec, Entrust, PGP and Computer Associates.

Category 16.3 Infrastructure protection & homeland security

2004-12-08 government homeland security cybersecurity support

NewsScan; http://www.washingtonpost.com/wp-dyn/articles/A45622-

2004Dec7.html

GROUP URGES GOVERNMENT TO FOCUS ON CYBERSECURITY

The Cyber Security Industry Alliance is calling on the Bush administration to beef up its cybersecurity operations, starting with elevating the position of national cybersecurity director to assistant secretary level. "There is not enough attention on cybersecurity within the administration. The executive branch must exert more leadership," says Alliance director Paul B. Kurtz, who's a former senior cybersecurity official in the Bush administration. Kurtz was joined by Amit Yoran, the former director of Homeland Security's National Cyber Security Division who resigned in September. Meanwhile, a provision in the recently passed intelligence overhaul bill that would have raised cybersecurity's profile in the Homeland Security Department was stripped out before passage. The Alliance's recommendations mirror those outlined in a report issued Monday by the House subcommittee on cybersecurity a top priority. In addition, both groups are urging the Homeland Security Department to take the lead in creating a disaster recovery and response plan, should the U.S. suffer debilitating digital sabotage. (Washington Post 8 Dec 2004)

# Category16.3Infrastructure protection & homeland security2004-12-10cybersecurity office Department of Homeland Security DHS IAIP CSIA proposal<br/>recommendation

DHS IAIP Daily; http://www.eweek.com/article2/0,1759,1739061,00.asp

December 10, eWeek — Cyber- security office moving ahead.

The office in charge of cyber- security in the Department of Homeland Security (DHS) is planning to continue moving ahead on the agenda the agency has already set. According to Lawrence Hale, deputy director of the National Cyber- Security Division at DHS, the agency considers physical and cyber- security so deeply intertwined that it would be impossible to separate them. Hale said the current organization of the IAIP (Directorate of Information Analysis and Infrastructure Protection) has cyber- security and physical security working together. Earlier this week, the CSIA (Cyber- Security Industry Alliance) released a series of recommendations, including a reorganization that would make the director of the cyber- security division an assistant secretary. Supporters say such a change would raise the profile of cyber- security, thus bringing the area more clout and more funding. While Hale said he thinks CSIA's proposals are an important means to raise the visibility of cyber- security, he doesn't agree that cyber- security should be treated differently from physical security. But he said he thought the CSIA meeting in Washington, DC where the recommendations were presented was helpful.

### 16.4 Military & government perspectives on INFOWAR

Category 16.4 Military & government perspectives on INFOWAR

#### 2004-02-27 virtual war games military exercises Navy battle

NewsScan

VIRTUAL WAR GAMES

Three aircraft carriers at Navy bases on both U.S. coasts are engaged this week in a virtual war game that uses computers to simulate battle conditions at sea. Vice Adm. Albert H. Konetzni Jr. says: "This will bring war-gaming to a new level. It will put the operators, the players, under great stress. They will be making decisions that are truly, truly critical to the carrying out of the operations, and it allows the operators, even down to the unit level, to really understand how they play in these scenarios." One of the participants in the exercise says: "We're trying to simulate all conditions of warfare that we could encounter: mine, surface, air, asymmetric threats like a small boat attack. All that stuff that could be damaging to the Navy is put forward into this war game." (San Jose Mercury News 27 Feb 2004)

Category 16.4 Military & government perspectives on INFOWAR

2004-04-23 cyber war game Army information warfare West Point NSA

DHS IAIP Daily;

http://www.reuters.com/newsArticle.jhtml?type=technologyNews &storyID=4897789&section=news

April 21, Reuters — Army confronts enemies within in cyber war game.

The mission: to secure an entire computer network for the United States and its allies against a vague enemy force. Hostile agents aim to wreak havoc on military plans, sabotaging databases, computer terminals and communications. But the cyber warriors planning a best defense aren't analysts hunkered down at the Pentagon. They are cadets at West Point competing against military academies and other schools in a four- day Cyber Defense Exercise this week. And the "enemy" isn't al Qaeda or Iraqi insurgents. It's a team led by none other than the National Security Agency (NSA). The NSA team, known as the "Red Cell," launches attacks on selected networks at the Air Force, Army, Coast Guard, Merchant Marine and Naval academies from an operations center somewhere in Maryland. The computer scenario plays out virtually inside the cadets' computers. Going on the offensive, or using so- called hackback techniques, is against competition rules. Also out- of- bounds are forms of sabotage in which computers can be turned into zombies and used to attack opponent machines with millions of data messages, shutting down communication.

Category 16.4 Military & government perspectives on INFOWAR

#### 2004-05-12 war games military academy NSA cyber defense

DHS IAIP Daily; http://www.gcn.com/vol1\_no1/daily- updates/25867- 1.html

May 12, Government Computer News — Merchant Marine Academy wins cybersecurity exercise.

The United States Merchant Marine Academy (USMMA) won out over four other service academies recently in a cybertraining exercise organized by the National Security Agency (NSA) and the United States Military Academy at West Point. During the Cyber Defense Exercise, a team of cadets from each academy had to design, build and configure a computer network that simulated a deployed joint services command. NSA and Department of Defense security experts tested the networks over a four- day period, attempting intrusions and identifying vulnerabilities. Teams were evaluated on maintaining services and their ability to recover from and prevent future security breaches, according to an NSA release. NSA found that the USMMA's network was stronger and more flexible then the 2003 champion, the U.S. Air Force Academy. Other teams participating were West Point, a former two- time winner; the U.S. Coast Guard Academy; and the U.S. Naval Academy.

Category16.4Military & government perspectives on INFOWAR2004-05-13broadband access bandwidth federal government DISA

DHS IAIP Daily; http://www.gcn.com/vol1\_no1/daily- updates/25882- 1.html

May 13, Government Computer News — DISA seeks bandwidth tech ideas.

The Defense Information Systems Agency (DISA) is seeking industry feedback on technologies that will add bandwidth to the Defense Information Systems Network (DISN). Under the DISN Access Transport Services request for information, released last week, the Defense agency is looking to industry for ideas to upgrade the older network at roughly 600 sites so it can be integrated with the \$900 million Global Information Grid- Bandwidth Expansion program. As part of the DISN upgrade, many legacy voice, data and video systems, as well as emerging capabilities—such as the department's premier network- centric warfare initiatives—will move to operate over IP. DISN currently operates via a switched- circuit transport system. According to the RFI, which closes on May 24, DATS will provide leased access transmission services between the government- owned backbone network and customer locations. The transmission services will be required to support bandwidths up through OC- 192. The DATS contract will provide similar services to two current DISA contracts that are expiring over the next two years, including the DISN Transmission Services CONUS (Continental United States) contract and the DISN Switched/Bandwidth Manager Services CONUS contract.

Category 16.4 Military & government perspectives on INFOWAR

#### 2004-05-17 computer security US army military network defense

DHS IAIP Daily;

http://www.fcw.com/fcw/articles/2004/0517/news- army- 05- 17- 04 .asp

May 17, Federal Computer Week — Army- wide security plan takes shape.

The Army will devise a servicewide computer security plan to boost protection of its information technology assets, according to Army and industry officials. Army officials say they want to develop a strategy that treats all systems as part of a cohesive enterprise, rather than securing each system individually. They realized the need for such a plan when they began taking an enterprise approach to managing their hardware and software, officials said. Their participation in military network defense groups also raised their awareness about the importance of cybersecurity, they said. Top Army IT officials, citing Army policies, would not confirm that their networks have seen more cyberattacks during the past five months. "The military typically experiences increases in computer network attacks when the geopolitical climate is the way it is," said Lt. General Steve Boutelle, the Army's chief information officer.

# Category16.4Military & government perspectives on INFOWAR2004-08-04cyber terrorism information asymmetrical warfare China Russia US Homeland<br/>Security concern

DHS IAIP Daily;

http://www.usatoday.com/tech/news/2004-08-02-cyber-terror\_x.htm

August 04, USA TODAY — Cyberterror impact, defense under scrutiny.

A coordinated cyberattack against the U.S. could topple parts of the Internet, silence communications and commerce, and paralyze federal agencies and businesses, government officials and security experts warn. Such an attack could disrupt millions of dollars in financial transactions, hang up air traffic control systems, deny access to emergency 911 services, shut down water supplies and interrupt power supplies to millions of homes, security experts say. But from whom the attacks would come is unclear. Intelligence shows al Qaeda is more fixated on physical threats than electronic ones, government officials and cybersecurity experts say. That hasn't dissuaded other groups and nations from eyeing cyberterrorism as a means to damage the U.S., whose infrastructures are increasingly tied to the Internet. "There are a large number of threats: hackers, cybercriminals, other countries," says Amit Yoran, director of the Department of Homeland Security's National Cyber Security Division. "It goes beyond al Qaeda." More than two dozen countries, including China and Russia, have developed "asymmetrical warfare" strategies targeting holes in U.S. computer systems. Because of U.S. military firepower, those countries see electronic warfare as their best way to pierce U.S. defenses, military experts say.

Category 16.4 Military & government perspectives on INFOWAR

### 2004-10-04 Korea INFOWAR information warfare hackers

NewsScan; http://news.ft.com/cms/s/3d592eb4-15f0-11d9-b835-00000e2511c8.html

SOUTH KOREA VULNERABLE TO CYBER ATTACKS FROM NORTH

South Korea's defense ministry says that North Korea has trained hundreds of computer hackers who could launch a cyber-war on South Korea, the US or Japan. Because South Korea has the world's highest usage of broadband services yet maintains relatively low levels of Internet security, the country is especially vulnerable to network attacks.

Category 16.4	Military & government perspectives on INFOWAR
---------------	---

### 2004-10-04 North Korea international Level 1 cyberwarfare 500 trained computer hackers

DHS IAIP Daily; http://www.channelnewsasia.com/stories/afp\_asiapacific/view/109911/1/.html

October 04, Agence France Presse — North Korea ready to launch cyber war: report.

North Korea has trained more than 500 computer hackers capable of launching cyber warfare against the United States, South Korea's defense ministry says. In a report to the National Assembly's National Defense Committee, the ministry said that hackers from North Korea were among the best in the world.

### Category 16.4 Military & government perspectives on INFOWAR

### 2004-10-20 US Canada NORAD security role join forces marine cyber security collaboration

DHS IAIP Daily; http://www.alertnet.org/thenews/newsdesk/N20568513.htm

October 20, Reuters — U.S., Canada seen broadening NORAD security role.

The United States and Canada are considering expanding their joint aerospace command to cover maritime and and cyber- security, U.S. Ambassador Paul Cellucci said on Wednesday, October 20. The North American Aerospace Defense Command (NORAD) was established to protect against Soviet bombers and was activated during the September 11 attacks on the United States, but it needs to take on a broader mandate, Cellucci said. "We believe that NORAD, which has been there for over 40 years protecting the airspace ... that in the age we live in we also have to be very concerned about marine security (and) cyber- security," he said.

Category 16.4 Military & government perspectives on INFOWAR

#### 2004-10-21 international cyberterrorism possibility 2006

DHS IAIP Daily; http://news.zdnet.co.uk/internet/0,39020369,39170864,00.htm

October 21, ZDNet (UK) — Cyberterrorism a possibility in two years.

Cyberterrorism could become a reality in 2006, a leading UK information security expert has said. Speaking at the SC Magazine Conference in London on Thursday, October 21, director of information security for Royal Mail David Lacey said that that the world would witness cyberterrorism within two years. Lacey said, "there is a lot of consistency in research that shows many of the real risks won't come to a crescendo until then. We know a lot about some of the trends coming. Real terrorists have not had the capability to carry out threats. But that will change as the stakes get higher." Source:

Category	16.4	Military & government perspectives on INFOWAR	

2004-11-12 DARPA military intelligence counterintelligence war ideas computer information warfare

DHS IAIP Daily;

http://www.fcw.com/fcw/articles/2004/1108/web- darpa- 11- 12- 04 .asp

November 12, Federal Computer Week — DARPA wants info about war ideas.

Defense Advanced Research Projects Agency (DARPA) officials want ideas on using computational techniques to disrupt enemy leaders' decision- making processes. DARPA officials want papers on the topic by December 10. They will choose the best ones and ask the authors attend a meeting in late January 2005. Military officials' growing emphasis on information warfare precipitated the request. Notice posted at: http://www2.eps.gov/spg/ODA/DARPA/CMO/SN05%2D09/Synopsis.htm l

### 16.5 Hacktivism

Category 16.5 Hacktivism

### 2004-05-19 hacking government hacktivism patriot hacker Internet Web security

DHS IAIP Daily; http://www.securityfocus.com/news/8717

May 19, Security Focus — 'Patriot' hacker pleads guilty.

A Florida man pleaded guilty in federal court in Washington DC, on Wednesday, May 19 to charges stemming from his role as one- half of the high- profile hacking team "The Deceptive Duo," responsible for obtaining sensitive information from government systems, and defacing dozens of government and private Websites with patriotic messages exhorting the U.S. to shore up cyber defenses. In a plea agreement with prosecutors, Benjamin Stark, 22, admitted to cracking eleven computer networks belonging to nine U.S. government departments and private commercial entities. The Deceptive Duo drew public attention in April 2002. As part of the plea, Stark admitted to working with an unnamed partner to crack systems at the Federal Aviation Administration (FAA), the Federal Highway Administration, the Defense Logistics Agency; the Department of Defense's Health Affairs office, the Department of Energy's Sandia National Lab, the Naval Air Systems Command, the Air Force Publishing Office, Dynamic Systems Inc. and Midwest Express.

Category 16.5 Hacktivism

#### 2004-05-20 Athens 2004 Olympics cyberattacks defense

DHS IAIP Daily; http://software.silicon.com/security/0,39024655,39120825,00.

htm

May 20, — Athens Olympics braced for wave of cyberattacks.

The Athens Olympics organizers are bracing themselves for a wave of cyberattacks once the games are under way, but insist that a physical breach of security still represents the biggest threat. Although questions remain about whether some of the venues will be ready for August 13, the IT planning is on course with a second technical rehearsal using some of the venues and simulating the four busiest days of the games taking place on June 14. By the start of the games some 200,000 people- hours of testing will have been completed and 10,000 defects are expected to be found and corrected. The infrastructure itself is fairly tried and tested with a policy of keeping complexity and risk down by only introducing new technology where it is essential. As such the platforms of choice are Unix and Windows, with Linux not getting a look- in.

Category 16.5 Hacktivism

#### 2004-07-14 Web hacktivism vandalism South Korean government Website China origin

NewsScan

### SOUTH KOREAN GOVERNMENT SITES ATTACKED

South Korea's spy agency says important government data may have been stolen during a spate of recent cyber-attacks launched from China. The attacks were considered a serious threat to South Korea's national security and the Chinese government has been urged to carry out its own investigation. Hackers using information-stealing viruses had broken into 211 computers at ten government agencies, including the Korea Institute for Defense Analyses and the Agency for Defense Development involved in weapons development. In addition, 67 computers at private companies, universities and media firms were hacked. (The Age 14 Jul 2004) Rec'd from John Lamp

Category 16.5 Hacktivism

#### 2004-07-20 Web hacktivism vandalism Chinese hackers Taiwan military Website

NewsScan

VANDALS ATTACK TAIWAN WEBSITE

Suspected Chinese hackers have launched an offensive against the website of Taiwan's Military News Agency ahead of practice freeway landings by fighter jets on the island. The hackers replaced the agency's homepage with a slogan that said 'Reunification with Taiwan in 2021' in an attack identical to one that occurred a month ago when suspected Chinese hackers attacked the site of Taiwan President Chen Shui-bian's pro-independence Democratic Progressive Party. Hong Kong's pro-Beijing Wen Wei Po daily last week quoted Chinese military sources as warning that Taiwan must re-enter the Chinese fold or face military action within the next 20 years. (The Age 20 Jul 2004) Rec'd from John Lamp

Category 16.5 Hacktivism

### 2004-08-04 Japanese government Websites attack hacktivism

DHS IAIP Daily; http://securityfocus.com/news/9274

August 04, Associated Press — Japanese government's computers hit by cyber attacks.

A wave of cyber attacks disrupted Japanese government computer networks earlier this week, but no damage was reported, an official said Thursday, August 5. The attacks, late Sunday and early Tuesday, targeted eight ministries and agencies and caused computers to freeze up under a deluge of data, Chief Cabinet Secretary Hiroyuki Hosoda told a news conference. Hosoda said the barrage also made it impossible for anybody to access Websites for the eight government bodies- - the Cabinet Office, Foreign Ministry, Finance Ministry, Justice Ministry, National Police Agency, Defense Agency, Coast Guard and Fair Trade Commission. "We don't know where the attack came from, or who did it," he said.

Category 16.5 Hacktivism

### 2004-08-25 political Websites electronic e-jihad Israel

DHS IAIP Daily; http://www.eweek.com/article2/0,1759,1639243,00.asp?kc=EWRSS 03119TX1K0000594

August 25, eWeek — Some concerns over electronic jihad.

Russian security researcher Yevgeny Kaspersky of Kaspersky Labs International said Wednesday, August 25, that a number of Arabic and Hebrew language Websites contained an announcement of an 'electronic jihad' against Israel to start on Thursday. However, Kaspersky stressed that such information was not necessarily trustworthy. "The e- jihad has been discussed for years, but an undisputed attack has yet to surface," said Ken Durham, director of malicious code at iDefense Inc. But Durham said security pros are increasingly worrying about when political activists might join with like- minded security and Internet programmers. While Kaspersky's warning appears to suggest wide- scale DDoS (distributed denial of service) attacks, experts suggested that important Internet services, as well as its root servers, are also at risk. For example, a DDoS attack in June against Akamai Technologies Inc. slowed traffic across the Internet for several hours. And in July, DoubleClick Inc.'s DNS (domain name system) was attacked and unable to serve ads for a similar time frame.

### 17.1 **Penetration**

Category17.1Penetration2004-03-17hacking attack penetration announcement California disclosure law

### NIPC/DHS

March 12, Security Focus - Hosting company reveals hacks, citing disclosure law.

Citing California's security breach disclosure law, Texas- based Allegiance Telecom notified 4,000 Web hosting customers this week of a March 3 computer intrusion that exposed their usernames and passwords. The law, called SB 1386, took effect July 1, 2003. It obligates companies doing business in California to warn their customers in "the most expedient time possible" about any security breach that exposes certain types of information: specifically, customers' names in association with their social security number, drivers license number, or a credit card or bank account number. Attorneys have warned that SB 1386 applies to e- commerce companies nationwide if they house information on residents of California. The intrusion did not directly expose information covered by the law, according to the company. Instead, the intruder pilfered thousands of passwords protecting customers' Web hosting accounts. Because many of those accounts are held by e- commerce companies, Allegiance issued the notice anyway, informing clients that SB 1386 may now oblige them to pass on the warning to their California customers if they accept personally identifiable information.

# Category 17.1 Penetration 2004-03-25 security breach source code penetration Gnome project Linux open-source operating system desktop

### NIPC/DHS

March 23, CNET News.com — Server breach likely to delay Gnome.

The Gnome Project administrators said Tuesday, March 23, that its servers have apparently been breached, potentially delaying the latest release of its desktop system for Linux. Gnome provides one of the two major desktop systems used on computers running the Linux operating system. "We are investigating further and will provide updates as we know more," Owen Taylor, a member of the Gnome system administration team said. The message also stated that the administrators believed the source code repository, which contains the current development work on Gnome software, was unaffected by the breach. The next version of the software, Gnome 2.6, will likely be delayed a few days while the project members investigate the breach. The software was scheduled to be released on Wednesday.

Category 17.1 Penetration

### 2004-04-13 network computer attack vandals TeraGrid Unix security incident National Science Foundation NSF

NewsScan

#### UNIVERSITY SUPERCOMPUTERS ATTACKED BY VANDALS

Network vandals have infiltrated supercomputers at as many as 20 colleges, universities and research institutions in recent weeks, disrupting the TeraGrid, a network of computers funded by the National Science Foundation and used in support of such scientific projects as weather forecasting and genome sequencing. The vandals have not been identified. None of the systems was permanently damaged, but the intruders gained the ability to control the various networks for short periods of time, prompting TruSecure security expert Russ Cooper to warn, "This could be a wake-up call to what should be very, very secure computing environments, because these machines should never have been compromised." The attacks were made against Unix machines. Stanford University computer security officer Tina Bird comments: "This incident is definitely giving us an opportunity to reevaluate the maintenance and protection we provide to our Unix systems. When you're completely focused on widespread attacks on Windows systems, it's certainly startling." (Washington Post 13 Apr 2004)

# Category 17.1 Penetration 2004-09-30 US government govt. Department of Energy DoE cybersecurity penetration hacking cracking report

DHS IAIP Daily; http://www.gcn.com/vol1\_no1/daily- updates/27489- 1.html

September 30, Government Computer News — DOE cybersecurity penetrated.

Weaknesses in the Department of Energy (DOE) cybersecurity allowed hackers to penetrate its systems 199 times last year, affecting 3,531 systems, the DOE's inspector general (IG) said. DOE continues to have difficulty finding, tracking and fixing previously reported cybersecurity weaknesses quickly, the IG said in a report, "The Department's Unclassified Cyber Security Program—2004."

### Category 17.1 Penetration

### 2004-10-21 Purdue University computer system penetration hack password changes information disclosure

DHS IAIP Daily; http://www.indystar.com/articles/7/188156- 5277- 102.html

October 21, Associated Press — Purdue computer system hacked.

Someone gained unauthorized access to Purdue University's computers, prompting school officials to urge all students, staff and faculty to change their passwords. "We have confirmed that some computer passwords have been obtained by unauthorized users accessing a number of computer systems," said Scott Ksander of Purdue's information technology office. The school has not been able to determine whether personal information was copied by the hacker.

### 17.2 Web vandalism

Category 17.2 Web vandalism

### Web vadalism network hacking al-Qaeda hostage beheading video

2004-06-19 NewsScan

NETWORK VANDALS POST TERROR VIDEOS ON INNOCENT WEB SITE

Network vandals invaded the Web site of a San Jose mapping and land-surveying company last week to post videos of the American engineer Paul Johnson, who was captured and later beheaded by al-Qaeda terrorists in Saudi Arabia. Tim Redd, owner of Silicon Valley Land Survey, said: "The

usage at the Web hosting company went sky-high. We're saddened by the events that provoked all this activity." Redd didn't know that vandals were using his Web site until a reporter from German magazine Der Spiegel contacted him. The FBI is investigating. Ira Winkler of the security firm CSC thinks it will be difficult to trace the invaders because they "will break into a series of networks and use them to disguise their tracks." (AP/USA Today 19 Jun 2004)

Category 17.2 Web vandalism

#### 2004-06-21 hacker Web vandalism South Korean defense site Trojan Horse attack

NewsScan

HACKER HITS SOUTH KOREAN DEFENSE

A network vandal has broken into computers at sensitive South Korean research institutes and government agencies, infecting more than 60 PCs with a variation of the Peep Trojan program. The National Cyber Security Center (NCSC) said the hacker had broken into computers at the Agency for Defense Development, which develops weapons, the Korea Atomic Energy Research Institute, the Korea Institute for Defense Analysis and three other government agencies. (The Australian 21 Jun 2004) Rec'd from John Lamp

Category 17.2 Web vandalism

#### 2004-06-23 Web vandalism Taiwan political site Chinese

NewsScan

HACKERS ATTACK TAIWAN RULING PARTY WEBSITE

Suspected Chinese hackers have attacked the website of Taiwan President Chen Shui-bian's pro-independence Democratic Progressive Party (DPP). The party's homepage was replaced with pro-China pictures and digitally altered images of Chen and his Vice President Annette Lu, a DPP official said. One photo shows a Chinese People's Liberation Army soldier aiming his rifle at a

target while another shows two men raising the Chinese national flag. Another picture shows Chen's head transposed onto the body of a man clad in traditional Japanese costume of kimono while Lu was transplanted onto an unclothed woman. (The Age 23 Jun 2004)

### 17.3 Phreaking, cramming, uncapping, theft of services

Category 17.3	Phreaking, cramming, uncapping, theft of services		
2004-02-05	cable modem hacking firmware flash Motorola coders limitations breach of contract illegal theft services	uncappers band	width
RISKS; http://www	v.securityfocus.com/ news/7977	23	18
CABLE MODEM HA (Kevin Poulsen, Secur	ACKERS CONQUER THE CO-AX ityFocus)		
firmware for a populai easier for uncappers ai communications. The 350 to 400 times a day Surfboard line, where cable modem a priv TCNiSO. With about community speed-h imposed by service pr- it makes it simple to cl anonymous service us	Ind of hobbyists steeped in the obscure languages of embedded syste of brand of cable modem, along with a technique for loading it a devide a service squatters, and threatens to topple long-held assumptions all program, called Sigma, was released in its final version last month, a ever since. It's designed to be flashed into the nonvolatile memory of it runs in parallel with the device's normal functionality. It gives user ilege previously reserved for the service provider. The project is the ten active members worldwide, the group is supported by contributi ungry Internet users who rely on TCNiSO's research and free hackwas oviders, usually in violation of their service agreement, if not the law, hange the modem's configuration file the key to uncapping, and, or ing "unregistered" modems. "I've known TCNiSO for two years now te a Canadian uncapper in an e-mail interview. "Sigma is the greatest	velopment that's alrea bout the privacy of ca nd has reportedly bee of certain models of I is almost complete co work of a gang of coo ions from the uncapp are to surmount the I To them, Sigma is a in some systems, to ge w and I've done a lot	ady made life able modem en downloaded Motorola's ontrol of their ders called bing bandwidth caps delight, because etting free
Category 17.3	Phreaking, cramming, uncapping, theft of services		
2004-02-12	organized crime cramming fraud telephone bills		
RISKS; http://www	v.nytimes.com/2004/02/11/nyregion/11MOB.html	23	
OFFICIALS SAY MO	DB STOLE \$200 MILLION USING PHONE BILLS		
	, >New York organized crime figures reportedly bilked millions of us		ers out of more

than \$200 million over five years by piggybacking bogus charges on their telephone bills ("cramming"). <

Category 17.3 Phreaking, cramming, uncapping, theft of services

2004-07-13 penetration criminal hacking phreaking

NYT http://www.nytimes.com/2004/07/13/nyregion/13hacker.html

Julia Preston of the New York Times wrote:

"A Westchester County man illegally infiltrated an internal computer at Verizon more than 100 times this year, forcing the telecommunications company to spend at least \$120,000 to retool its security system, prosecutors charged in a federal indictment yesterday [Monday 12 July 2004].

The man, William Quinn, 27, of Eastchester, obtained many passwords to a central computer that Verizon technicians use in repairing telephone lines, according to the indictment, filed in the Southern District of New York in Manhattan.....

Category 17.3 Phreaking, cramming, uncapping, theft of services

#### 2004-07-20 phone phreaking Phillipines hacking telecommunications Manila raids

NewsScan

THREE HELD ON PHREAKING CHARGE IN PHILLIPINES

Eight people, including two Indians, a Bangladeshi, and five Filipinos, have been arrested for allegedly hacking into Philippines telecommunications systems to make unauthorized long-distance calls. The suspects, who were arrested in a series of raids in and around Manila, will be charged with

using computer equipment to break into the systems of corporate subscribers of dominant carrier Philippine Long Distance Telephone Co. and then selling long-distance calls to other people, charging the costs to the unwary corporate subscribers. (The Age 20 Jul 2004) Rec'd from John Lamp

### **18.1** Theft of equipment

Category 18.1 Theft of equipment

2004-05-03 NIC physical security theft loss of service

DHS IAIP Daily; http://www.eweek.com/article2/0,1759,1583359,00.asp

May 03, eWeek — Network card theft causes Internet outage.

The theft of network cards from a Verizon central office in New York has caused some customers there to lose their Internet access. A handful of corporate customers were left without e- mail and Internet access Monday, May 3, after the theft of networking equipment from a New York City office Sunday, May 2. Law enforcement officials said four DS- 3 cards were reported missing from a Manhattan co- location facility owned by Verizon Communications Inc. The outage affected area customers of Sprint Corp. "We found backup cards in the area," said Charles Fleckenstein, spokesperson for Sprint in Overland Park, KS. "All of the cards are now on site in New York. [They] are being installed at this moment." Service was being restored to customers as the cards were being installed, he said. Sprint officials said other ISPs were affected by the incident, but declined to identify them. Verizon spokesperson Dan Diaz would not identify which providers were affected by the theft of the equipment. Diaz said no Verizon Internet customers were affected by the outage.

Category 18.1 Theft of equipment

2004-05-17 theft telecom physical security

DHS IAIP Daily; http://www.eweek.com/article2/0,1759,1593073,00.asp

May 17, eWEEK — New York theft raises questions.

As of late last week, local and federal investigators were proceeding with their probe into a burglary at a Midtown Manhattan telecommunications office. According to the New York City Police Department, three DS- 3 networking cards were stolen May 2 from a New York central office (CO) of Verizon Communications Inc. This CO, also a co- location office housing competing carriers' equipment, is one of the many hubs for the country's voice and data networks and a key component of the nation's critical infrastructure. "Everybody's overly sensitive, with reason, to the issues of terrorism or terrorists trying to sabotage the infrastructure, whether it be the Brooklyn Bridge or the Internet," Joseph Valiquette, spokesperson for the New York FBI Field Office, said about the involvement of the FBI's Joint Terrorism Task Force in the Verizon burglary. The online operations for several New York- based businesses were shut down for almost an entire business day as a result of the Verizon theft.

Category 18.1 Theft of equipment

2004-08-05 hacker theft fraud indictment Romania shipment conspiracy

DHS IAIP Daily; http://www.informationweek.com/story/showArticle.jhtml?artic leID=26806085&tid=13692

August 05, InformationWeek — Hacker indicted on equipment theft charges.

A federal grand jury in Los Angeles on Wednesday, August 4, indicted a Romanian hacker and five Americans on charges that they conspired to steal more than \$10 million in computer equipment from Ingram Micro Corp.. The 14- count indictment charges that Calin Mateias, who used the online nickname "Dr. Mengele," hacked into Ingram Micro's ordering system beginning in 1999 and placed fraudulent orders for computer equipment. When Ingram Micro subsequently blocked shipments directed to Romania, he allegedly recruited the co- defendants named in the indictment to provide U.S.- based addresses as mail drops for fraudulently ordered equipment. If convicted, Mateias faces up to 90 years in prison.

### 18.2 Loss of equipment

Category 18.2 Loss of equipment 2004-05-04

hackers theft damage data loss Taiwan

### DHS IAIP Daily;

http://www.chinapost.com.tw/taiwan/detail.asp?ID=48429&GRP=B

May 04, The China Post — Hackers cause almost one million dollar loss for banks, CIB reveals.

Hackers have invaded the computer systems of over 700 Taiwan companies and caused losses of more than USD\$900,000 for banks with electronic financial services, according to an initial estimate by the Criminal Investigation Bureau (CIB). In the field of computer hacking, CIB officials said mainland China is the major source of hackers targeting Taiwan with the aim of stealing commercial secrets, technical know- how, and computer systems of government agencies in charge of military, transport, public security, and finance affairs. Other sources include the United States, Japan, and South Korea. Officials said the hackers normally implant malicious programs in the form of "Trojan Horse" viruses onto the less guarded Internet operating systems of educational institutions like schools. The virus and software programs then wait for opportunities to enter the systems of other organizations with more stringent security. Companies suffering from the attacks include information service companies, high- tech firms, enterprises in the traditional manufacturing industries, and banks with Internet services. The dozens of banks reported that over USD\$600,000 million was lost in the electronic fund transfer process.

### **19.1 Software piracy**

Category 19.1 Software piracy

### peer-to-peer P2P software piracy Kazaa Morpheus economic loss

2004-01-19 NewsScan

PEER-TO-PEER SOFTWARE THEFT

Peer-to-peer (P2P) file-sharing programs like Kazaa are increasingly being used for software piracy; in fact, William Plante of the security company Symantec thinks that roughly half of the illegal copies of his company's software are made through P2P electronic downloads. The thieves are "truly ghosts on the Internet" who are "virtually untraceable." One approach to curbing software piracy is mandatory online activation, and even though Plante admits those methods can be broken, he says it's "extremely inconvenient to try and use the cracked version." Michael Weiss of StreamCast Networks, which makes the P2P program Morpheus, says the software industry should get an entirely new attitude, which would "embrace the technology, just like the movie studios ended up embracing VCR's. This is not going to go away. Technology always wins out. You would think the software companies would know that more than Hollywood." (New York Times 19 Jan 2004)

# Category 19.1 Software piracy 2004-02-14 Microsoft source code Windows XP NT online Internet intellectual property rights issues

NewsScan

STOLEN CODE RAISES SECURITY CONCERNS

The distribution on the Internet of stolen source code for portions of Microsoft's Windows 2000 and Windows NT operating systems is raising new concerns among security experts. A former federal computer crime prosecutor says, "This raises real national security concerns. The fact that Microsoft's software is so widely available will have an impact across the computer security industry." Critics have often accused Microsoft of doing a poor job of protecting the security of its software from network vandals. A Microsoft executive's response to the latest theft was: "We take this seriously. It's illegal for third parties to post or make our source code available. From that standpoint we've taken appropriate legal action to protect our intellectual property." (New York Times 14 Feb 2004)

# Category 19.1 Software piracy 2004-07-07 Business Software Alliance BSA theft piracy copyright infringement statistics one third

NewsScan

STOLEN: ONE THIRD OF THE WORLD'S SOFTWARE

The Business Software Alliance, a trade group, says that 36% of all the software in the world has been pirated, costing the industry \$29 billion in lost revenue. The five countries with the highest incidence of pirated software are: China (92%), Vietnam (92%) and Indonesia (88%), Ukraine (91%), and Russia (87%). (AP/San Jose Mercury News 7 Jul 2004)

# Category 19.1 Software piracy 2004-08-24 software piracy law enforcement police crackdown music video films copyright infringement plagiarism

NYT http://www.nytimes.com/reuters/technology/tech-crime-poland-hackers.html?th

Polish police arrested members of a large software-piracy gang accused of stealing and selling music and videos.

The criminals stored their materials on large computer systems at universities around the world and may also have stolen theses from these computers for sale in plagiarism services.

### Category 19.1 Software piracy

2004-09-16 Federal Bureau of Investigation FBI illegal pirated software seize Digital Marauder

DHS IAIP Daily; http://www.infoworld.com/article/04/09/16/HNfbi\_1.html

September 16, InfoWorld — FBI seizes \$87 million worth of illegal software.

A two- year investigation by U.S. law enforcement authorities has resulted in one of the largest seizures of fake software ever in the U.S. and charges against 11 individuals. The defendants from California, Washington, and Texas were indicted, Wednesday, September 15, with conspiring to distribute counterfeit computer software and documentation with a retail value of more than \$30 million, the U.S. Attorney's Office for the Central District of California said in a statement. The value could rise to \$87 million, U.S. Attorney's Office spokesperson Thom Mrozek said. When arresting the defendants and searching their homes, offices and storage facilities, Federal Bureau of Investigation agents uncovered an additional stockpile of more than \$56 million worth of fake Microsoft Corp., Symantec Corp. and Adobe Systems Inc. products. Microsoft worked closely with the authorities in Los Angeles on the case, which was code- named "Digital Marauder."

### Category 19.1 Software piracy

### 2004-11-03 hackers software piracy source code club Cisco PIX firewall Enterasys IDS Usenet email sales

DHS IAIP Daily; http://www.pcworld.com/news/article/0,aid,118452,00.asp

November 03, IDG News Service — Hackers reopen online store.

An anonymous group of malicious hackers has reopened an online store that sells the stolen source code of prominent software products. The Source Code Club is offering the code for Cisco Systems' PIX firewall software to interested parties for \$24,000, according to messages posted in online discussion groups. The group is using e- mail and messages posted in a Usenet group to communicate with customers and receive orders for the source code of several security products, including Cisco's PIX 6.3.1 firewall and intrusion detection system (IDS) software from Enterasys Networks, the group says. Cisco did not immediately respond to a request for comment.

Category 19.1 Software piracy

### 2004-11-12 SQL theft Microsoft software piracy intellectual property

NewsScan; http://australianit.news.com.au/articles/0

FOUR IN COURT OVER SQL THEFT

Four former Microsoft employees have been charged with stealing \$32 million worth of software and selling it on the side. According to a complaint filed by Microsoft, the workers ordered software available to Microsoft employees for free to use for business purposes, then sold it to online software retailers. The complaint said the employees blocked managers from getting routine email notification that the workers were ordering the software. The software the four are accused of stealing included the SQL Server 2000, which normally sells for \$15,000, and the SQL Enterprise Server 7.0, which sells for \$29,000. (The Australian, 12 Nov 2004)

Category 19.1 Software piracy

#### 2004-11-24 Microsoft Windows XP piracy countermeasure Counterfeit Project

DHS IAIP Daily; http://www.vnunet.com/news/1159640

November 24, VUNet — Microsoft gets tough with XP pirates.

Microsoft has moved to clamp down on software pirates in the UK after discovering what it describes as a large volume of high quality counterfeit versions of Windows XP. The software maker has invited "anyone unsure as to the legitimacy of their Windows XP software" to submit their products for analysis. Software that is found to be counterfeit will be replaced for free subject to the terms and conditions of its offer, Microsoft promised. The XP Counterfeit Project marks the latest in a series of moves by Microsoft to target software pirates.

### **19.2 Music piracy**

Category19.2Music piracy2004-01-04RIAA lawsuits piracy deterrent

NewsScan

ONLINE PIRACY BEGAN TO DISSIPATE AFTER RIAA THREATENED LAW SUITS

A new study by the Pew Internet & American Life Project shows that the number of music downloaders fell in the past six months from 29% to 14% — and suggests that the drop-off was a consequence of the Recording Industry Association of America's plans to sue Internet users suspected of trading pirated music over file-sharing networks. RIAA Chairman Mitch Bainwol says: "This is another data point that tells us in fact that the lawsuits have had an enormous impact on public awareness about the legality of downloading. For some the prospect of getting sued is a pretty effective deterrent. For most folks, just understanding that it was illegal is enough." (Washington Post 4 Jan 2004)

Category 19.2 Music piracy

### 2004-01-05 copyright piracy MP3 internet music downloading

NewsBits; http://www.nytimes.com/2004/01/05/business/media/05song.html

Songwriters Say Piracy Eats Into Their Pay

David Bernstein wrote about the effects of music piracy on songwriters in a January 5, 2004 article in the New York Times. Songwriters' income depends largely on royalties from album sales; with the drop in such sales as a result of widespread theft of music tracks, writers have seen their income decline. For example, veteran songwriter Charles Strouse, 75, saw his income drop by 50% between 2002 and 2003 due to piracy. Typically, writers receive a few pennies for every copy of their music sold; with 2B illegal downloads per month displacing sales, their revenues are seriously affected. Many writers have lost steady jobs at music-publishing companies and are looking for other work.

Category 19.2 Music piracy

2004-01-22 **RIAA lawsuits illegal file sharing copyright infringemnet intellectual property rights** 

NewsScan

PROVING IT'S SERIOUS, RIAA FILES NEW LAWSUITS

The Recording Industry Association of America (RIAA), the music industry trade group, has filed lawsuits against 532 people it's accusing of illegally sharing music downloaded from the Internet. The lawsuits are intended to show that the recording industry's drive against downloaders will continue. RIAA says: "Our campaign against illegal file-sharing is not missing a beat. We can and will continue to bring lawsuits against those who illegally distribute copyrighted music on peer-to-peer networks." (San Jose Mercury News 22 Jan 2004

### Category 19.2 Music piracy

### 2004-01-27 record labels bypassed MUDDA legal download

NewsScan

MUSICIANS BYPASS RECORD LABELS WITH NEW ONLINE VENTURE

Rock veterans and Internet enthusiasts Peter Gabriel and Brian Eno are launching a musician's alliance next month that aims to cut the middlemen out of the music sales process by promoting online sales by musicians directly to their fans. The alliance, dubbed the "Magnificent Union of Digitally Downloading Artists" or MUDDA, would allow musicians to set their own prices and agendas, free from the artificial confines of the CD format. Gabriel says he's not trying to shut down the record labels, but wants to give artists more options, building on the success of legitimate download sites such as Apple's iTunes music store. "I'm an artist who works incredibly slowly. If some of those [songs] could be made available, you don't have to be so trapped into this old way of being confined only by the album cycle," says Gabriel. (AP/Los Angeles Times 27 Jan 2004)

# Category 19.2 Music piracy 2004-02-11 file music sharing digital piracy anonymous AnonX Kazaa copyright intellectual property rights peer-to-peer Vanavatu

NewsScan

### ANONYMOUS SERVICE MASKS FILE-SWAPPERS

Wyatt Wasicek, a programmer whose day job is working for an Internet service provider, is offering music downloaders who use file-sharing programs such as Kazaa a way to do so anonymously. His service, AnonX, is available for \$5.95 a month and provides protection by setting up a virtual private network between the user's computer and the company's servers. The AnonX computers act as proxies, so that the actual users' identities are masked. Wasicek has promised not to divulge the e-mail addresses of his 7,000 subscribers and says he doesn't think he can be forced to do so because AnonX's official owner lives in Vanuatu, the Pacific island nation that also hosts Kazaa's parent company, Sharman Networks. AnonX's servers are located overseas as well. Wasicek says he decided to create AnonX to shield the occasional file-sharer who's unaware of copyright infringement ramifications. "I'm doing this to protect the family with the 13-year-old, not the 25-year-old with 25 movies he's sharing with his buddies. I wanted to go back to the good old days when people could surf anonymously," says Wasicek. (AP 11 Feb 2004)

Category	19.2	Music piracy
----------	------	--------------

### 2004-02-17 **RIAA lawsuits file music sharing intellectual property rights copyrights**

NewsScan

RIAA FILES 531 MORE LAWSUITS AGAINST FILE-SHARERS

The Recording Industry Association of America has filed five separate lawsuits against 531 Internet users that it accuses of illegal file-sharing. The action comes on the heels of four similar suits filed by the RIAA against 532 users last month. All the suits are using the "John Doe" method, which identifies the alleged song-swappers through their numerical Internet addresses. The RIAA is seeking to discover the swappers' names and addresses through court-issued subpoenas. An appeals court in December ruled in favor of Verizon that the RIAA could not force ISPs to divulge the identities of subpoena targets before the lawsuits were filed. Sarah Deutsch, VP and associate general counsel for Verizon, says it has not yet received any subpoenas during this go-round, but is interested to see whether briefs filed by the Electronic Frontier Foundation and American Civil Liberties Union protesting RIAA's tactics will affect the case. "We're waiting for the resolution of the due process issues that have been raised by the public interest groups," says Deutsch. Meanwhile, Nielsen SoundScan, which tracks U.S. music sales, says U.S. album sales are up 10.4% this year compared to the same period in 2003. (Reuters/New York Times 17 Feb 2004)

Category 19.2 Music piracy

#### 2004-02-18 **RIAA countersued New Jersey woman scare gang tactics**

NewsScan

#### TABLES TURNED ON RIAA — ACCUSED FILE-SWAPPER FIGHTS BACK

A New Jersey woman has countersued the Recording Industry Association of America, accusing it of extortion and racketeering tactics in its strategy to sue individual file-sharers. Michele Scimeca's lawsuit is one of "a handful" of countersuits, according to the RIAA. "If someone prefers not to settle, they of course have the opportunity to raise their objections in court," says an RIAA spokesperson. "We stand by our claims." Scimeca contends that by suing file-swappers and then settling the cases before they're brought to trial while threatening potential liabilities that could reach into the hundreds of thousands of dollars, the RIAA is engaging in activities more often associated with gangsters and organized crime. "This scare tactic has caused a vast amount of settlements from individuals who feared fighting such a large institution and feel victim to these actions and felt forced to provide funds to settle these actions instead of fighting," says Scimeca's attorney. "These types of scare tactics are not permissible and amount to extortion." The RIAA has sued a total of about 1,500 people and has settled with 381 of those. (CNet News.com 18 Feb 2004)

## Category19.2Music piracy2004-03-04intellectual property rights copyright music piracy file sharing peer-to-peer P2P<br/>Kazaa office raids Australia

NewsScan

KAZAA RAIDS GET GREEN LIGHT

Australia's federal court has dealt a blow to locally based file-sharing network Kazaa, allowing music industry lawyers and investigators access to material seized in raids on the company's headquarters. The court dismissed an application by Kazaa owner Sharman Networks to have the civil search orders that permitted the February 6 raids stayed, ruling that major record companies should be allowed to examine documents and computer files taken in raids on Sharman's offices and the homes of several executives of the company. (The Australian 4 Mar 2004, rec'd from John Lamp, Deakin University

Category 19.2 Music piracy

2004-03-10 peer-to-peer P2P legal music download Napster IBM Superpeer college student

NewsScan

NAPSTER, IBM TARGET COLLEGES WITH NEW DIGITAL MUSIC SYSTEM

Napster took the wraps off a new "Super Peer" application, which uses IBM's eServer BladeCenter systems to store the most popular music tracks in on-site servers rather than on the Internet. The "Super Peer" application is being marketed to colleges and universities as a way to reduce their computing infrastructure's vulnerability to overuse. Citing usage statistics at Penn State, for instance, of 100,000 downloads and 100,000 streams per day, Napster CTO Bill Pence says storing the most popular songs on-site could save the university an estimated \$50,000 in bandwidth fees the first year: "When we embarked on our industry-leading university program, we set out to alleviate the technical and business strains that illegal file-sharing puts on universities and ISPs." (Reuters/Washington Post 10 Mar 2004)

Category 19.2 Music piracy

### 2004-03-23 lawsuit raid Kazaa offices intellectual property rights peer-to-peer P2P file music sharing

NewsScan

SEARCH 'MESS' DELAYS KAZAA CASE

The music industry will have to wait until at least May before being granted access to material seized in raids on the headquarters of peer-to-peer network Kazaa. An Australian federal court judge has described the execution of civil search orders as "a bit of a mess," and ordered the seized material held until May. These materials include documents and computer files taken in raids on the office of Kazaa owner Sharman Networks and the homes of several key executives. (The Australian 23 Mar 2004)

Category 19.2 Music piracy

2004-03-30 music industry internation lawsuit illegal file music sharing peer-to-peer P2P

NewsScan

MUSIC INDUSTRY TARGETS EUROPEAN FILE-SHARERS

The International Federation of the Phonographic Industry has filed lawsuits against 247 people in Denmark, Germany, Italy and Canada, and warns of "further waves of lawsuits against major offenders" in coming months. The actions in Germany and Italy alleged criminal copyright infringement activity, because a criminal designation is required in order to obtain names from Internet service providers. The lawsuits are aimed primarily at large-scale file-sharers, with one case in Denmark allegedly involving more than 50,000 songs, according to IFPI chairman and CEO Jay Berman. The music industry has blamed piracy, both online and physical, for contributing to a decline in music sales over the past few years, from \$38 billion in 1998 to \$30 billion in 2003. In Denmark, CD sales have slipped by about 50% in the past four years. "The stealing has got to stop," says Johan Schluter, secretary general of the Danish Recording Industry Association. "Record stores are closing down, and artists find it increasingly difficult to get their music released." (Wall Street Journal 30 Mar 2004)

### Category19.2Music piracy2004-04-01file-sharing peer-to-peer P2P Kazaa effect music sales

### NewsScan

### KAZAA OWNER WELCOMES SURVEY FINDINGS

Sharman Networks, owner of the Kazaa peer-to-peer software, has been quick to seize on the findings of a survey released in the U.S. on Monday which concluded that downloading music had no effect on album sales. In a media release issued last evening, Sharman chief executive Nicola Hemming said "We welcome sound research into the developing peer-to-peer industry and this study appears to have covered some interesting ground. The findings certainly support the vision we've always held for Kazaa and crystallizes our vision for the future of content distribution." The 2002 study was conducted jointly by researchers from Harvard Business School and the University of North Carolina, Chapel Hill, and used data from file-sharing services with 1.75 million downloads being studied over 17 weeks in autumn 2002. "Consider the possibilities if the record industry actually cooperated with companies like us instead of fighting," Ms. Hemming said. "We've offered content providers the opportunity to work with peer-to-peer customers for nearly two years, yet the record industry continues its narrow-minded strategy of litigation and legislation. (The Age, 31 March 2004, rec'd from John Lamp, Deakin University)

#### Category 19.2 Music piracy

### 2004-04-08 copyright music intellectual property rights copy-protected CD

NewsScan

SOFTWARE BYPASSES CD ANTI-COPYING PROTECTION

A new software program developed by German computer magazine c't (Computertechnik) and RapidSolution Software takes a decidedly low-tech approach to bypassing the copy-protection technologies that some music companies are including in their CDs. UnCDcopy works by recording the analog output from a regular CD player and automatically reconfiguring the analog file into digital format, splitting the file into separate tracks just like the original. The quality of the UnCDcopy version is significantly less than that of a digital copy, but will still work. "This is like CD to tape copying, only brought into the 21st century," says Jim Peters, a representative of the UK's Campaign for Digital Rights. "It will let you defeat any copy prevention system, but in an obvious low-tech way." (New Scientist 8 Apr 2004)

## Category 19.2 Music piracy 2004-04-19 music sharing copyright infringement RIAA amnesty program downloaders disbanded

NewsScan

#### RECORDING INDUSTRY DISBANDS AMNESTY PROGRAM

The Recording Industry Association of America (RIAA) has terminated a program that offered to shield individuals from being sued by recording companies if they admitted to illegally sharing music online. Only 1,108 people signed up for amnesty program since it was launched last September, and the RIAA has now filed court papers indicating that the program is no longer necessary or appropriate, and is withdrawing it. Fred von Lohmann of the Electronic Frontier Foundation says the program "was sort of a sham from the beginning," because the RIAA has no way of keeping an individual copyright holder from suing any of the individuals who signed up for it. "The headlines for the amnesty program have dissipated and now it's pretty clear that their main goal is to use the stick of litigation." (AP/San Jose Mercury News 19 Apr 2004)

Category 19.2 Music piracy

2004-04-21 flie-swapping blocker Palisade Systems peer-to-peer P2P copyrighted content

NewsScan

PALISADE LAUNCHES FILE-SWAPPING BLOCKER

Palisade Systems is launching software that can identify and block copyrighted songs from being traded online. The software, created by Audible Magic, has received support from the recording industry as well as the interest of some higher education institutions who are seeking to gain control over the file-swapping activities of their students. "They want to take the position of not filtering out all peer-to-peer (traffic), stopping copyrighted works but not the other content," says Palisade founder Doug Jacobson. The Audible Magic technology will be included as an option in the newest version of Palisade's PacketHound network-management services. The technology sits inside a network and checks e-mails and other peer-to-peer transfers for audio "fingerprints" that match its database of copyrighted music files. If found, the technology blocks the file transfer midstream. (CNet News.com 21 Apr 2004)

### Category19.2Music piracy2004-04-23Napster backing venture copyright infringement intellectual property rights

### NewsScan

NAPSTER-BACKING VENTURE FIRMS HIT WITH LAWSUIT

Universal Music and EMI Group have filed a copyright infringement lawsuit against Hummer Winblad Venture Partners and two partners — John Hummer and Hank Barry — alleging that the venture capital group contributed to unauthorized copying of music through its \$13 million investment in Napster and through Barry's role as Napster's CEO for more than a year. Both men also served on Napster's board. The suit seeks \$150,000 per copyright violation plus punitive damages. "Businesses, as well as those individuals or entities who control them, premised on massive copyright infringement of works created by artists should face the legal consequences for their actions," said the two record labels in a joint statement. Hummer Winblad's investment was made in May 2000 — after the recording industry sued Napster for enabling copyright infringement, but the case never made it to trial. Napster filed for bankruptcy protection in June 2003. The National Venture Capital Association is watching the case closely and cautioned that the outcome could have a chilling effect on investment in unproven technologies, thus hampering economic growth. "The concern is that investors are being sued for investing in high-risk companies," says NVCA VP Jeanne Metzger. (Reuters 23 Apr 2003)

### Category19.2Music piracy2004-04-27music piracy bootlegging encouraged David Bowie artist mash-ups prizes

NewsScan

BOWIE CALLS ON BOOTLEGGERS

David Bowie has invited fans to bootleg his music -- and he's offering prizes for the most creative theft. The musician's Web site invites fans to mix classic Bowie songs with material from his latest album, "Reality" to create a "mash-up" -- a track superimposing the vocal line from one song with the backing tracks from another. The technique has long been employed by record producers, but music software has made it accessible to thousands of "bedroom DJs" - to the alarm of record companies battling to control the distribution of music through the Internet. Bowie, 57, was quoted in The Times, saying mash-ups were "a great appropriation idea waiting to happen." "Being a hybrid maker off and on over the years, I'm very comfortable with the idea and have been the subject of quite a few pretty good mash-ups myself," he said. (The Australian, 27 Apr 2004, rec'd from John Lamp, Deakin University)

Category 19.2 Music piracy

2004-05-07 anonymouse file-sharing music MP2P peer-to-peer RIAA

NewsScan

TRULY ANONYMOUS FILE-SHARING

Pablo Soto, co-founder of Madrid-based Optisoft, which runs the music-only file-sharing networks Blubster and Piolet on proprietary MP2P peer-to-peer platform, says: "Our users are requesting more and more privacy. They are more than disgusted with the threat of lawsuits." Soto says a new system upgrade should protect Optisoft's users from legal action brought taken by the music trade group the Recording Industry Association of America (RIAA), which has sued a number of Internet users for putting their music collection online for others to download. Soto says, "I do not think it will stop the RIAA from suing our users. But if any of our users has the balls to go to court, I don't see any way on the planet for the RIAA to win." (Reuters/USA Today 7 May 2004)

# Category 19.2 Music piracy 2004-07-27 music sharing allowed permitted legal service MusicMatch Napster copyright infringement peer-to-peer

NewsScan

LIMITED SHARING ALLOWED BY MUSIC SERVICES

MusicMatch is the latest online music service to provide a feature that lets subscribers send e-mail messages with Internet links for songs they want to share. Although Napster 2.0 and other licensed digital music services offer similar options, Napster allows nonsubscribers to listen only

to 30-second song snippets, whereas MusicMatch allows songs to be played by recipients three times before the songs lock. MusicMatch executive Bob Ohlweiler says, "Record companies like the fact that people can tell their friends and acquaintances about music. What the labels don't like about

peer-to-peer is that it's free." Media analyst Phil Leigh says of the limited file-sharing feature: "It will be an incremental feature that could lead them to be more competitive. You'll probably see other people follow MusicMatch's lead, particularly if it proves successful, and my guess is that it will be." (AP/San Jose Mercury News 27 Jul 2004)

### Category 19.2 Music piracy

### 2004-07-30 disc jockey DJ record store music piracy copyright infringement intellectual property rights violation case lawsuit payment Australia

NewsScan

DJS ORDERED TO PAY IN MUSIC PIRACY CASE

The Federal Court of Australia has ordered five disc jockeys, a record store and its director to pay a total of \$140,000 to the owners of copyright, whose music they had copied and sold. The award was in favor of Universal Music, Sony Music Entertainment (Australia) and Warner Music Australia. The DJs who were asked to pay go by the names Moto, Chocolate Boy Wonder, Peter Gunz, Demo, and Tikelz. Record store Anthem Records and its director Joe Sitoa were also asked to pay. The respondents had produced and distributed compilation CDs containing music from some of the biggest names in rhythm and blues, including Ja Rule, Jennifer Lopez and Missy Elliot. (The Age, 30 Jul 2004) rec'd from John Lamp, Deakin U.

### Category 19.2 Music piracy

### 2004-08-05 file sharing peer-to-peer software music piracy copyright infringement encryption law evasion US state attorney general

NewsScan

STATES TO FILE-SHARING COMPANIES: WATCH OUT

Most of the country's state attorneys general have sent a warning letter to seven companies that promote online file-sharing software such as Kazaa and Morpheus, warning them that there could be legal consequences if they don't adequately inform computer users about the potential risks of using their software. The letter also urged the companies not to add encryption features to their software to hide users' identity: "Encryption only reinforces the perception that P2P technology is being used primarily for illegal ends. Accordingly, we would ask you to refrain from making design changes to your software that prevent law enforcement in our states from investigating and enforcing the law." Adam Eisgrau of P2P United, a trade group that represents several of the firms, says: "Asking us not to use encryption is incredibly shortsighted when there are clear legitimate corporate and public uses for a private network." Fred von Lohmann of the Electronic Frontier Foundation in San Francisco says of the letter: "I'm not aware of any state law that file-sharing violates. This letter is clearly an exercise of political clout on the part of the entertainment industry." (AP/San Jose Mercury News 5 Aug 2004)

# Category19.2Music piracy2004-08-20file sharing music peer-to-peer software copyright law infringement intellectual<br/>property rights Sony Betamax

NewsScan

COURT ON FILE-SWAPPING: GET USED TO IT

A three-judge panel of the 9th Circuit Court of Appeals has ruled that the movie and recording industries can't stretch copyright law to block online piracy of songs and movies. If the decision is appealed, the U.S. Supreme Court could revisit its landmark Sony Betamax ruling that protected

from copyright lawsuits products that have substantial legitimate uses. Whereas the same appeals court ruled against file-sharing service Napster in 2001 because it stored illegally copied files on its central computers, today's peer-to-peer file-sharing networks have no central computers -- and

cannot even monitor users, let alone control them. The court urged the entertainment industry to adapt to file sharing the way movie studios did after losing the Betamax case: "The introduction of new technology is always disruptive to old markets, and particularly to those copyright owners whose

works are sold through well-established distribution mechanisms. History has shown that time and market forces often provide equilibrium in balancing interests, whether the new technology be a player piano, a copier, a tape recorder, a video recorder, a personal computer, a karaoke machine or an MP3 player." (Los Angeles Times 20 Aug 2004)

# Category19.2Music piracy2004-08-23anti-download file sharing peer to peer copyright infringement intellectual property<br/>rights student college university

NewsScan

UNIVERSITIES BEEF UP ANTI-DOWNLOADING TACTICS

Many U.S. universities are greeting returning students with tighter restrictions on using campus networks for illegal music downloading and file-swapping. Until recently, universities had relied on a soft approach -- lecturing students on copyright issues and making them sign pledges to abstain from illegal downloading -- but many are now taking a more hardline stance. Virginia State University recently installed network firewalls that block download sites such as Kazaa and eDonkey -- a move that officials say instantly reduced bandwidth usage from 95% to 51%. The University of Nevada at Las Vegas has installed technology that automatically deletes files saved to communal computers whenever the machines are turned off. "We're not content police. We're bandwidth police," says UNLV associate provost Lori Temple. "We make it so downloading music is a horrible idea." And the University of Florida has developed its own software, Icarus, to detect

illegal downloading by scanning network traffic for peer-to-peer files. A first violation cuts off the student's for 15 minutes -the second time, the penalty goes up to five days. Meanwhile, other schools are taking the carrot approach, striking deals with legitimate music services, such as the

reincarnated Napster, to offer free or very inexpensive access to streamed music. All these measures are necessary, say college administrators, in order keep their schools off the RIAA's growing lawsuit list. (Wall Street Journal 23 Aug 2004)

### Category 19.2 Music piracy

2004-08-24 anti-piracy copyright infringement music file sharing university efforts RIAA praise intellectual property rights

#### NewsScan

UNIVERSITIES PRAISED FOR ANTI-PIRACY EFFORTS

Cary Sherman, president of the Recording Industry Association of America (RIAA), says he's pleased with recent efforts by academic institutions to curb illegal copying of copyrighted material: "It's quite clear that every university has gotten the message that this is a serious issue and they're all doing something." At least 20 universities (including Penn State, the University of Miami, and Northern Illinois University) have signed deals with such licensed download services such as Napster 2.0, Ruckus, and RealNetworks to provide students with discounted downloading of free music streaming. (AP/San Jose Mercury News 24 Aug 2004)

Category 19.2 Music piracy 2004-08-26

http://www.nytimes.com/2004/08/26/technology/26share.html

FBI officers raided six peer-to-peer network operators participating in an illegal file-sharing operation called the "Underground Network."

Investigators infiltrated the network and, according to Saul Hansell, writing in the New York Times, "downloaded 84 movies, 40 software programs, 13 games and 178 songs from the network."

Category 19.2	Music piracy
2004-09-20	Wire magazaine CD experiment artist copyright free copyleft rip burn share
	distribute peer-to-peer intellectual property rights

NewsScan

STEAL THIS MUSIC

The editors of Wired magazine have compiled a CD whose contents are meant to be shared, copied, remixed and sampled in an experiment aimed at supporting the Creative Commons concept of intellectual property licensing. About 750,000 copies of "The Wired CD: Rip. Sample. Mash. Share" will be mailed along with Wired's November issue and the disc will also be distributed to audience members at a benefit concert headlined by David Byrne, whose "My Fair Lady" appears on the CD. Other artists include the Beastie Boys, Zap Mama and Gilberto Gil. "The artists were relatively easy to get on board," says Wired editor-in-chief Chris Anderson. "The labels have different priorities. Some of them, once briefed, got it, and some of them never really saw the advantages." Anderson says he approached 50-60 artists in order to come up with the 16 featured on the CD. (Wall Street Journal 20 Sep 2004)

### Category 19.2 Music piracy

### 2004-09-27 music industry Recording Industry Association of America RIAA legal tactics lawsuits overpriced micropayments MP3

NewsScan < http://www.msnbc.msn.com/id/6037780/site/newsweek/>

MUSIC INDUSTRY SHOULD CHARGE LESS, SELL MORE

The music industry is fighting a losing battle, says Newsweek columnist Steven Levy, who says the RIAA's legal tactics make about as much sense as trying to sue a hurricane: "Technology generates its own form of nature, a set of conditions that enforce an artificial, yet equally unstoppable, reality... For the longest time, the labels viewed digital music as something that could hurt them with hurricane force but made no efforts to adjust to this new reality, let alone exploit it." Levy notes that Real Networks' experiment with sharply cutting prices for digital music -- to 49

cents per song -- was a losing proposition because they still owed 70 cents in royalties for each song sold. But what's impressive is that Real sold six times as much music and took in three times as much money as when they had prices pegged at the industry's 99-cent standard. Levy says that if

labels and artists would agree to smaller royalties, everyone could get richer quicker: "Behind Door One is the money you can make by selling a million copies of a tune. Behind the other door is the money to be reaped by selling 6 million copies at half the price. Do the math, guys!" Not only

that, but lowering prices significantly might just stamp out the scourge of pirated music -- and that's what the labels say they want, right? (Newsweek 27 Sep 2004)

Category 19.2 Music piracy

#### 2004-10-04 copy protection Sony music piracy

NewsScan; http://www.siliconvalley.com/mld/siliconvalley/9832592.htm

DECLARING VICTORY, SONY ABANDONS COPYRIGHT PROTECTED CDs

Sony's music unit will no longer be selling CDs that use built-in technology to prevent their being copied, because the company has come to the conclusion that its message against illegally copying of CDs has become widely accepted. Sony's persistent dilemma has been how to protect the copyrights on its movies, music and other entertainment assets while at the same time making its electronics devices attractive to consumers.

### Category 19.2 Music piracy 2004-10-12 file swapping piracy music RIAA supreme court loss SCOTUS Supreme Court ISP Internet Service Provider DMCA Digital Millennium Copyright Act extension

NewsScan; http://www.washingtonpost.com/wp-dyn/articles/A26513-2004Oct12.html

SUPREME COURT TURNS DOWN INTERNET PIRACY CASE

The Recording Industry Association of America has lost a round in its ongoing efforts to use the courts in its battle against online music piracy. The U.S. Supreme Court on Tuesday turned down a request to settle a dispute over whether Internet service providers can be forced to identify subscribers accused of illegally swapping music and video files. Lawyers for Verizon, which had sought to keep subscribers' information private, argued that the recording industry has been quite successful in going after people who trade copyrighted works, having sued more than 3,000 alleged infringers in the past 10 months. The issue turns on the provisions of the 1998 Digital Millennium Copyright Act, which was written before the problem of file-swapping was common. An appeals court earlier ruled that it's up to Congress, not the courts, to expand the law to cover popular file-sharing networks. This latest decision is separate from a petition filed last week by the recording industry asking the Supreme Court to hold Grokster and Streamcast Networks responsible for their customers' file-swapping activities.

Category 19.2 Music piracy

### 2004-10-27 mp3 RIAA iTunes Napster Musicmatch RealNetworks

NewsScan; http://news.com.com/From+gold+records+to+gold+MP3s/2100-1027 3-5429377.html

SIGN OF THE TIMES: GOLD MP3s

In a nod to the digital age, the Recording Industry Association of America has issued its first gold, platinum and multiplatinum certifications for digital downloads. RIAA chief executive Mitch Bainwol calls the awards "a reflection of both the commitment of the entire music community to consumer-friendly legitimate digital services and fan appetite for high-quality music." The RIAA based its certifications on sales from legitimate digital download services, including Apple iTunes, Musicmatch, Napster and RealNetworks. And the winner is: Outkast's "Hey Ya!" with more than 400,000 downloads (earning it the only multiplatinum designation). In addition, six songs qualified for platinum (200,000 downloads) and 45 for gold (100,000 downloads). (CNet News.com 27 Oct 2004)

Category 19.2 Music piracy

### 2004-12-06 music piracy Kazaa Grokster artist

NewsScan; http://www.nytimes.com/2004/12/06/arts/06down.html

ARTISTS LOVE THE WEB, HATE MUSIC PIRACY

In the first large-scale survey of artists (i.e., filmmakers, writers and digital artists), musicians and the general public, the Pew Internet and American Life Project has found that only about half of the artists polled thought that sharing unauthorized copies of music and movies online should be illegal. Nearly two-thirds of those said filesharing services such as Kazaa and Grokster should be held responsible for illegal fileswapping, while only 15% thought it was a good idea to go after individual users. Among musicians, 37% said the file-sharing services and users should share the blame for illegal file-swapping, while 17% singled out the services as the guilty parties. The survey results indicate that while file-swapping is an ongoing irritant to artists and musicians who see their work distributed for free on the Net, they also value the widescale exposure that the Internet makes possible. "The overall picture is that the musician-artistic community has a much wider range of views and experiences than folks who watch the Washington debate about copyright might imagine," says Lee Rainie, director of the Pew Internet Project. (New York Times 6 Dec 2004)

### **19.3** Movies / TV piracy

Category 19.3 Movies / TV piracy

### intellectual property rights copyrights FBI warning CDs DVDs

2004-02-19 NewsScan

FBI WARNING LABELS TO APPEAR ON CDs, DVDs

The Federal Bureau of Investigation is giving Hollywood film studios, music companies and software makers permission to use the FBI's name and logo on various digital media to deter consumers from making illegal copies. FBI official Jana Monroe says, "This anti-piracy seal should serve as a warning to those who contemplate the theft of intellectual property, that the FBI will actively investigate cyber crimes and will bring the perpetrators of these criminal acts to justice." Unauthorized copying and distribution of digital content is punishable by up to five years in prison and a fine of \$250,000. (Los Angeles Times 19 Feb 2004)

Category 19.3	Movies / TV piracy
2004-07-12	Internet usage South Korea movie piracy illegal download films high-speed access
N	

NewsScan

S.KOREA: 3 OF 5 INTERNET USERS ILLEGALLY DOWNLOAD FILMS

About one-fourth of Internet users in an eight-country survey admit to illegally downloading movies but the percentage is more that twice as high in South Korea. According to a survey by the Motion Picture Association of America (MPAA), an average of 24% of Web users in the eight countries have downloaded at least one movie, and in South Korea (a country with the highest percentage of Internet users on high-speed connections) the number was 58%. Since downloading a movie over high-speed connections takes just a few minutes, the MPAA fears that piracy will grow as more Internet users boost their speed. (The Age 12 Jul 2004) Rec'd from John Lamp.

 Category
 19.3
 Movies / TV piracy

 2004-08-04
 DVD piracy copying copyright infringement intellectual property rights lawsuit company shutdown

NewsScan

DVD-COPYING COMPANY SIGNS OFF

321 Studios, which has been embroiled in lawsuits brought by deep-pocketed movie studios and video game producers, has quietly given up the ghost. In a posting on the 321 Web site it announced "it has ceased business operations including, but not limited to, the sale, support and promotion of our products." Tuesday's announcement came on the heels of another legal setback when a New York federal judge imposed a worldwide ban on the production and distribution of 321's Games X Copy software in response to a lawsuit by three leading makers of video games. 321 has steadfastly maintained that its copy software was merely intended for consumers who prefer to make backups of expensive DVDs and video games in case of damage to the originals. (AP/Washington Post 4 Aug 2004)

Category 19.3	Movies / TV piracy
2004-08-10	DVD software company MPAA copyright infringement intellectual property rights financial settlement lawsuit

NewsScan

DVD SOFTWARE COMPANY YIELDS TO MPAA

Software company 321 Studios in St. Louis will stop selling DVD copying software worldwide and has agreed to a financial settlement with the Motion Picture Association of America (MPAA). MPAA chief executive Jack Valenti says: "321 Studios built its business on the flawed premise that it could

profit from violating the motion picture studios' copyrights; the courts have been amply clear -- there is no leniency for violating federal copyright laws. Now that the company's illegal copying software is off of store shelves worldwide, we have moved to settle the case." In addition, Valenti warned: "This is not the end of the story in our massive fight against piracy." (AP/San Jose Mercury News 10 Aug 2004)

## Category 19.3 Movies / TV piracy 2004-10-05 fraud piracy music movies anti-counterfeiting initiative Homeland Security US government

DHS IAIP Daily;

http://www.washingtonpost.com/wp- dyn/articles/A7331- 2004Oct4 .html

October 05, Washington Post — Anti- counterfeiting initiative launched.

On Monday, October 4, four U.S. agencies announced a coordinated attack to stem the global trade in counterfeit merchandise and pirated music and movies, an underground industry that law- enforcement officials estimate to be worth \$500 billion each year. The effort, known as the Strategy Targeting Organized Piracy (STOP), includes stepping- up border enforcement to intercept fake goods as they are entering the United States, targeting the earnings of traders of counterfeit goods and publicizing the names of overseas companies that traffic in counterfeit products. Joining the campaign are U.S. Trade Representative Robert B. Zoellick, the Justice Department, the Commerce Department and the Department of Homeland Security, which includes the customs and border- protection bureau.

Category 19.3 Movies / TV piracy

2004-10-12 US federal task force piracy crackdown intellectual property rights protection

DHS IAIP Daily;

http://www.washingtonpost.com/wp- dyn/articles/A27583- 2004Oct 12.html

October 12, Associated Press — U.S. authorities call for piracy crackdown.

A federal task force has recommended expanded investigative and prosecutorial powers to combat intellectual property theft ranging from counterfeit drugs to swapping songs over the Internet. Wiretaps should be allowed to investigate intellectual property theft that threatens health and safety and more investigators should be added in key U.S. cities and in piracy hot spots in Asia and Eastern Europe, the report released Tuesday, October 12 said. The report also endorsed the rights of companies to compel Internet service providers to turn over the names of people who have traded songs, movies, software or other copyright- protected items over the Internet. Piracy costs American companies \$250 billion per year, the report estimated. Report: http://www.usdoj.gov/criminal/cybercrime/IPTaskForceReport.p df

Category 19.3 Movies / TV piracy

### 2004-11-04 movie piracy Hollywood MPAA video lawsuits litigation education criminal prosecution copyright infringement

NewsScan; http://www.latimes.com/technology/la-fi-mpaa4nov04

HOLLYWOOD LAUNCHES ANTI-PIRACY CAMPAIGN

Taking its lead from major record companies, Hollywood studios have prepared a host of lawsuits against people who illegally use copyrighted movies obtained via filesharing networks. Dan Glickman, president of the Motion Picture Association of America (MPAA), says that what's needed to combat piracy is "a holistic approach" -- including educational efforts, criminal prosecution, and lawsuits against infringers. "You need the stick and you need the carrot both. You can't just have one without the other." But film producer Ross Grayson Bell says that the industry's focus should be on providing legal ways to buy movies on the Internet -- and that Apple iTunes Music Store is the right model because it lets people download songs quickly and at a reasonable price: "There is a need that is not being met. I think the real way to curb piracy is to take away that need. The industry has to present a viable way to see movies in this new age." (Los Angeles Times 4 Nov 2004)

### Category19.3Movies / TV piracy2004-11-05Hollywood movie piracy MPAA RIAA lawsuits videos copyright infringement

NewsScan; http://online.wsj.com/article/0

HOLLYWOOD THREATENS LAWSUITS AGAINST ONLINE PIRATES

The Motion Picture Association of America says its members are poised to file copyright-infringement lawsuits against digital movie downloaders, following the lead of the music industry, which has filed thousands of such lawsuits over the past year. But while the music industry has demonstrated decidedly mixed results, the movie industry may be more successful, in part because the campaign is getting underway while movie downloading is still relatively rare, representing only 2% of all online file sharing. "The studios have a little bit of a head start. By taking action now, [they] have a better chance in making a real dent in the problem," says one copyright attorney. One reason for the small number of film downloads is the size of the files -- users could download hundreds of songs in the same time it takes to download one movie. In addition, movie fans are not as disaffected with that industry, unlike music enthusiasts who resent paying \$15 for a CD with only one or two songs that they really want. "The deal between you and Hollywood is pretty good. The deal between you and the music industry has been pretty lousy for a long time," notes Eric Garland, CEO of BigChampagne. (Wall Street Journal 5 Nov 2004)

Category 19.3 Movies / TV piracy

### 2004-11-17 Hollywood MPAA movie piracy lawsuits Internet copyright infringement

NewsScan; http://news.bbc.co.uk/1/hi/entertainment/film/4018755.stm

HOLLYWOOD SUES INTERNET FILM PIRATES

The Motion Picture Association of America has filed an undisclosed number of lawsuits against Internet users it suspects of swapping or downloading digital copies of films. The group says the civil suits could seek damages of up to \$30,000 per film. The MPAA move follows a similar strategy by the music industry to crack down on illegal downloading, which resulted in about 5,000 lawsuits. MPAA Dan Glickman said in a statement: "The motion-picture industry must pursue legal proceedings against people who are stealing our movies on the Internet. The future of our industry, and of the hundreds of thousands of jobs it supports, must be protected from this kind of outright theft using all available means." (BBC News 17 Nov 2004)

Category 19.3 Movies / TV piracy

### 2004-12-15 MPAA Hollywood BitTorrent pirates copyright infrincgement lawsuits

NewsScan; http://www.usatoday.com/tech/news/2004-12-15-bittorrentsuits x.htm

HOLLYWOOD SUES "PARASITE" BITTORRENT USERS

Hollywood movie studios have filed copyright infringement lawsuits against the operators of computer servers that BitTorrent software to relay digital movie files across online file-sharing networks. John Malcolm of the Motion Picture Association of America (MPAA) says: "Today's actions are aimed at individuals who deliberately set up and operate computer servers and Web sites that, by design, allow people to infringe copyrighted motion pictures. These people are parasites, leeching off the creativity of others. Their illegal conduct is brazen and blatant." However, Fred von Lohmann, an attorney with the Electronic Frontier Foundation, warns: "By bringing these suits, the MPAA runs the risk of pushing the tens of millions of file sharers to more decentralized technologies that will be harder to police." (AP/USA Today 15 Dec 2004)

### **Games piracy** 19.5

Category 19.5 Games piracy 2004-06-11

### Valve Half-Life 2 game code theft arrest piracy hackers customer credit

NewsScan

ARREST MADE IN VIDEOGAME CODE THEFT

The FBI-led Northwest Cyber Crime Task Force has made arrests in "several countries" as part of its investigation into the theft of Valve Corp.'s Half-Life 2 videogame code last year. The task force declined to give details on the arrests, but Valve chief executive Gabe Newell credited a "core group" of the company's customers for sending and analyzing information that helped lead to the arrests. "Gamers were able to unravel what are traditionally unsolvable problems for law enforcement related to this kind of cyber-crime," says Newell. Following the theft, Valve was forced to rewrite parts of its programming, delaying the game's launch by almost a year from its original release date. Some industry insiders say the delay has caused something of a backlash against hackers. "Gamers really want to play Half Life 2, and they really, really resented the delay," says the founder of a videogame news site called GameSpot. Fan Darrin Schrader agrees: "It hurts the community when people do this. I just hate cheaters, and hackers are cheaters." (Washington Post 11 Jun 2004)

#### Category 19.5 Games piracy

#### 2004-11-08 video games piracy P2P peer-to-peer

NewsScan; http://apnews.excite.com/article/20041108/D867MSU80.html

PIRATES SEE VIDEO GAMES BEFORE PAYING CUSTOMERS DO

Pirated copies of the sci-fi action title "Halo 2" and games such as "Grand Theft Auto: San Andreas" and "Half-Life 2" have been circulating on file-sharing networks, news groups and Web sites even before their official release to consumers. Brian Jarrard of Microsoft's Bungie Studio, which produced "Halo 2," complains: "You spend three years of your life pouring everything you have into this project, and then somebody gets their hands on the game and gives it away to the world for free. We made this, and these guys had no right to give it out to the public." Douglas Lowenstein, president of the Entertainment Software Association, admits: "The problem and challenge with piracy is that there are people out there on a worldwide basis who've identified piracy as a very profitable enterprise. You don't end this problem overnight." (AP 8 Nov 2004)

# 19.7 Counterfeit legal or business documents

Category	19.7	Counterfeit legal or business documents	
Calegoly	10.7		

### 2004-01-10 anti counterfeit technology Adobe Photoshop

NewsScan

ADOBE ACKNOWLEDGES ANTI-COUNTERFEITING TECHNOLOGY

Adobe Systems admits that the latest version of its popular Photoshop graphics software includes technology that generates a warning message when someone tries to make a digital copy of some currencies. The technology was added at the request of government regulators and bankers and was designed by the Central Bank Counterfeit Deterrence Group, a consortium of 27 banks in the U.S., Canada, Europe and Japan. "We sort of knew this would come out eventually," says an Adobe spokesman. "We can't really talk about the technology itself." Angry consumers have flooded Adobe's message boards with complaints over censorship and concerns over future restrictions that could include adult-oriented or copyrighted material. "This shocks me," says the president of the Photoshop users group in San Diego. "Artists don't like to be limited in what they can do with their tools. Let the U.S. government or whoever is involved deal with this, but don't take the powers of the government and place them into a commercial software package." (AP/Washington Post 10 Jan 2004)

### 19.8 Plagiarism

Category 19.8 Plagiarism

2004-01-21 copyright law plagiarism university student

http://www.cnn.com/2004/LAW/01/21/ctv.plagiarism/

STUDENT WINS FIGHT AGAINST TURNITIN USE

A McGill University student refused to allow his professors to submit his essays to the Turnitin.com plagiarism checker on the grounds that it was violating his intellectual property rights. The senate committee reviewing his case agreed with him.

Category 19.8	Plagiarism
2004-02-05	electronic copyright distortion corruption modification attribution source Google search engine plagiarism authenticity

RISKS	23	18
PLAGIARISM TOO EASY		

Jim Griffith complained about the distortion of a 1997 article he wrote that was recently modified without his permission, stripped of attribution, and widely circulated and even printed in otherwise reputable astronomy publications. He wrote, "As moderator of RHF, I understand the difficulties of identifying the original source of a piece, and the ease with which people remove attributions. I'm disturbed by the casual way so many publications blindly printed the piece without doing a serious attempt to identify the source or the original version. Granted, that source isn't immediately obvious, but a reasonable Google search or a date-sorted Google Groups search would have definitively identified both the author and the original wording. In effect, Google Groups is now my primary hope for preserving my original copyright (although I did have the foresight to encode in the piece via e-mail, I'd now have no hope of ever claiming credit or preserving the original version." He added, "I'm mainly disturbed by the ease with which the original piece was corrupted, and that that corruption was blindly accepted and propagated. It is now the case that corrupted version is more prevalent than the original. This is disappointing, given that an advantage of electronic communications is supposed to be the way it preserves information. I wonder if we'll find that in a hundred years, the most popular Internet version of "Romeo and Juliet" is one with a new, happier ending?"

Category 19.8	Plagiarism
2004-04-06	plagiarism filters artificial intelligence pattern matching industry

NewsScan

PLAGIARISM SOFTWARE DETECTS NEW MARKET IN CORPORATE WORLD

Software designed to detect plagiarism is moving from academia, where it's been used for years to flag phony term papers, to the corporate world. Newspapers, law firms and even the U.N. Security Council are using the data-sifting tools to ensure their documents are original works, and companies such as iParadigm, Glatt Plagiarism Services, MyDropBox and CFL Software Development have moved quickly to meet the new demand. And while some businesses have been reluctant to deploy such software, iParadigm president John Barrie predicts that soon the number of corporate clients will outstrip academics. "The stakes are 100 times greater. We're not talking about grades anymore," he says. (AP/Washington Post 6 Apr 2004)

# 1A1 Criminal hacker conventions and meetings

# Category 1A1 Criminal hacker conventions and meetings 2004-08-03 Defcon 12 Meet the Feds presentation talk recruitment NSA US government criminal hacker

DHS IAIP Daily; http://www.pcworld.com/news/article/0,aid,117226,00.asp

August 03, PC World — Government seeks a few good hackers.

A well- attended session at the recent Defcon 12 hackers' conference in Las Vegas, NV, was "Meet the Feds," a recruitment presentation by a group of federal cybercrime law enforcement agents, who fielded questions from would- be cybercops. September 11, 2001, marked a turning point for government recruitment, says former NSA Director of Information Assurance Mike Jacobs, who now works in the private sector. Before the terrorist attacks, the NSA typically received about 200 applications monthly, he adds. In the three months following the attacks, more than 20,000 people applied for employment at the NSA. In the presentation, he urged computer- savvy patriots to put their skills to use defending the country from spies, terrorists, and other criminals. One hitch, of course, is a security clearance- - elusive for some hackers. Jim Christy, director of the Department of Defense's Cyber Crime Center, and Tim Huff, a special agent with the FBI's Computer Analysis Response Team, fielded questions about so- called gray- hat hackers, who sometimes break the law but aren't charged. Christy and Huff made it clear that cybercriminals- - even those who haven't been caught- - are not likely to be invited to join the ranks of cybercops.

Category 1A1	Criminal hacker conventions and meetings
--------------	--

### 2004-08-03 computer hacking contest Singapore HackAttack 2004

DHS IAIP Daily;

http://www.usatoday.com/tech/news/2004- 08- 03- singapore- hacke rs\_x.htm

August 03, Associated Press — Singapore to hold computer hacking contest.

Singapore said Tuesday, August 3, it would organize a contest to find the tech- savvy city- state's best computer hacker. Six pairs will compete in the August 20 "BlackOPS: HackAttack Challenge 2004," organized by the government- funded National Infocomm Competency Center, said its marketing manager Yvonne Choo. They will "penetrate, exploit, gain access and obtain privileged information from the other teams' servers, for the purpose of corporate espionage," the center said on its Website. Teams will also have to defend their organization's networks against hacking from other teams in the daylong event, it added. Choo said he hoped the contest would help shed light on ways to prevent actual computer attacks. The prize for the best hacker will be a DVD burner and free computer classes. Asia has been the root of some of the worst attacks by hackers in recent years. Close to 80% of Singapore's four million citizens own personal computers and the island is largely considered to be the most technologically advanced in Southeast Asia.

Category 1A1 Criminal hacker conventions and meetings

#### 2004-08-20 computer hacking contest Singapore HackAttack 2004 techniques

DHS IAIP Daily;

http://story.news.yahoo.com/news?tmpl=story&cid=562&ncid=738&e=7&u=/ap/20040820/ap\_on\_hi\_te/singapore\_hacking\_contest

August 20, Associated Press — Computer experts vie in hacking contest.

Twelve computer experts hunkered down Friday, August 20 for a seven- hour contest to find the best hacker in tech- savvy Singapore. Divided into six two- person teams, the contestants participating in "BlackOPS: HackAttack challenge 2004" have to defend their networks and servers from hacking while attacking other teams' systems. The contestants hailed from Brunei, China, Myanmar and Singapore, but their identities couldn't be revealed because they all work in the computer security business, organizers said. Teams were not allowed to use the Internet as a hacking tool, only computers and modems. Asia has been the root of some of the worst attacks by hackers in recent years. Singapore has said it is increasingly concerned about cyber security in the highly wired city- state where eight in 10 households own personal computers. Hackers can be jailed for up to three years or fined up to \$5,852 under Singapore's Computer Misuse Act. Organizers had said they hoped the contest would help shed light on ways to prevent actual computer attacks.

# 1A3 Biographical notes on individual criminals (including arrests, trials)

Category 1A3 Biographical notes on individual criminals (including arrests, trials)

2004-01-09hacking database New York Times loss jail

NewsScan

PRISON TERM FOR NETWORK VANDAL

Under a plea deal with federal prosecutors, a 22-year-old California man agreed to serve a prison term of six months to one year for hacking into a database of the New York Times. The database contained personal information about the newspaper's opinion/editorial page contributors, and the Times calculated that the intrusion caused it more than \$5,000 in losses. (Reuters/Los Angeles Times 9 Jan 2004)

Category 1A3 Biographical notes on individual criminals (including arrests, trials)

### 2004-02-14 virus writer Belgium arrest cyber crime 19-year-old student Gigabyte

DHS IAIP Daily; http://securityfocus.com/news/8048

February 14, Associated Press — Belgium police arrest female virus- writer.

Belgian police arrested a 19- year- old female technology student who gained international notoriety for creating computer viruses, it was reported Saturday, February 14. The woman, identified only by her nickname "Gigabyte," was charged with computer data sabotage under legislation introduced in 2000 to deal with cyber- crime, the daily La Libre Belgique reported. If convicted, she faces up to three years in prison and fines of up to \$127,000. Police reportedly released the woman after 24 hours, confiscated her five computers and shut down her Website. She was arrested Monday in her hometown of Mechelen, 20 miles north of Brussels. "She was preparing to publish new viruses on this site," Inspector Olivier Bogaert of the Belgium police was quoted as telling La Libre Belgique. Her youth and gender helped gain Gigabyte notoriety in the male- dominated world of computer hackers. In a 2002 interview Gigabyte defended her work, saying she herself never spread the viruses she created and published on her Website. "When people make guns, can you blame them when somebody else kills with them?" she was quoted asking. "I only write them. I don't release them."

Category 1A3 Biographical notes on individual criminals (including arrests, trials)

2004-03-12 music movie piracy case Australia extradition intellectual property rights issues

NewsScan

PIRACY EXTRADITION CASE ADJOURNED

A Sydney, Australia court is to decide if Hew Raymond Griffiths, 41, who is alleged to have headed an international software piracy ring known as "Drink or Die," should be extradited to face charges in the U.S. Griffiths had been indicted by a grand jury in the state of Virginia with one count of criminal copyright infringement and one count of conspiracy to commit criminal copyright infringement. If convicted he faces up to 10 years imprisonment and a \$500,000 (US) fine. Griffith's barrister argued the U.S. had not made out a case for extradition, having failed to prove dual criminality — that what his client allegedly did in the U.S. would also have been a crime in Australia. However, the Commonwealth DPP refuted that argument, saying it had made a valid case for extradition in relation to both criminal copyright and conspiracy. (The Australian 12 March 2004, rec'd from John Lamp, Deakin University)

Category 1A3	Biographical notes on individual criminals (including arrests, trials)
2004-03-25	federal wiretapping keylogger California arrest
NIDC /DUS	

### NIPC/DHS

March 23, Reuters — Feds charge California man for using keystroke logger.

A California man who prosecutors say planted an electronic bugging device on a computer at an insurance company was indicted on Tuesday, March 23, on federal wiretapping charges. Larry Lee Ropp, a 46- year- old former insurance claims manager, is the first defendant charged with a federal crime for using a "keystroke logger," which tracks the activities on a computer and feeds the information back to its owner, a spokesman for the U.S. Attorney's Office in Los Angeles said. Prosecutors did not say what they believe Ropp hoped to gain by bugging the computer, which was being used by a secretary to executives at the company where he worked, Bristol West Insurance Group. But an affidavit filed with the indictment suggests he intended to supply information to attorneys representing a class of people who were suing the company. Investigators were tipped to Ropp after he was fired from the company and asked another employee to remove the keystroke logger, which records every keystroke made on a computer, from the secretary's machine.

Category 1A3 Biographical notes on individual criminals (including arrests, trials)

2004-03-26 Internet blacmailer arrest Holland Netherlands Net-harm credit card fraud

NIPC/DHS

March 24, The Register — Dutch Internet blackmailer gets ten years.

A 46- year- old Dutch chip programmer who tried to blackmail dairy company Campina has been jailed for 10 years by a Dutch court on blackmail charges and five counts of attempted murder. The blackmailer put agricultural poison in Campina Stracciatella desserts in a bid to extort money. The man forced Campina to open a bank account and asked them to deposit \$242,750. Campina was issued with a credit card for the account which the blackmailer intended to use to withdraw the cash. But to avoid breaking cover, he asked Campina to buy a credit card reader and extract the information from the card's magnetic stripe. The output, together with the card's pin code, was sent to him electronically via steganography. Campina received an envelope containing a floppy with a stego program and some instructions. The company then had to encode the credit card data into a picture. The blackmailer downloaded the picture, decoded the information it contained, created his own copy of the card, and finally went to withdraw the cash. To download the online picture, he used the Anonymizer.com service, believing the company's privacy policy would protect him. However, he was caught red- handed last year when he withdrew the money from a cash machine using his copy of the credit card.

Category 1A3 Biographical notes on individual criminals (including arrests, trials)

2004-05-08 worm virus malicious code malware Microsoft Windows vulnerability Sasser

DHS IAIP Daily; http://www.chron.com/cs/CDA/ssistory.mpl/world/2558235

May 08, Reuters — Police: Microsoft helped catch suspect.

German police were led to the home of an 18- year- old man suspected of creating the "Sasser" computer worm after a tip- off from Microsoft, police said Saturday, May 8. Spokesman Frank Federau for Lower Saxony police said that German police were certain they had the man behind one of the Internet's most costly outbreaks of sabotage. "We are absolutely certain that this really is the creator of the Internet worm because Microsoft experts were involved in the inquiry and confirmed our suspicions and because the suspect admitted to it," he said. Microsoft had received anonymous tip- offs about the worm's creator and then contacted the FBI and German police, Federau said. All three worked together to find the suspect. The teenager's computers were confiscated by police but the suspect himself was not in custody, Federau said. Since appearing a week ago, Sasser has wreaked havoc on personal computers running on Microsoft Windows 2000, NT and XP operating systems, but is expected to slow down as computer users download anti- virus patches. The computing underground responsible for hatching worms and viruses has proved a difficult ring to crack for law enforcement and security experts were surprised at the rapid arrest.

Category 1A3 Biographical notes on individual criminals (including arrests, trials)

### 2004-05-13 agobot trojan author german sabotage worm computer malicious

NewsScan

SUSPECTED AGOBOT TROJAN AUTHOR ARRESTED

A 21-year-old German man has been arrested and charged under the country's computer sabotage law for creating the Agobot Trojan, a malicious computer worm. (This case is unrelated to the Sasser worm, which was also traced to a young German man). Five other Germans have also been charged in connection with the distribution of these Trojan programs. (The Age 13 May 2004) rec'd from John Lamp, Deakin U.

Category 1A3 Biographical notes on individual criminals (including arrests, trials)

2004-05-18 phishing email scam fraud

DHS IAIP Daily;

http://www.washingtonpost.com/wp- dyn/articles/A37406- 2004May 18.html

May 18, Washington Post — E- mail scammer gets four years.

An Internet scammer who used e- mail and a fraudulent Website to steal hundreds of credit card numbers was sentenced to almost four years in jail Tuesday, May 18, one of the stiffest- ever penalties handed down for online fraud. Houston, TX federal court Judge Vanessa Gilmore sentenced Houston resident Zachary Hill to 46 months in jail for his role in duping consumers into turning over 473 credit card numbers. Hill used a "phishing" scheme to make his e- mail look like it came from America Online, the nation's largest Internet service provider, or PayPal, the online 4 payment subsidiary of auction giant eBay. The message told victims that their accounts had lapsed and that the companies required their credit card numbers and passwords to restart them. Hill prompted recipients to enter their information into Web forms designed to look like pages run by the companies, the Justice Department said. Hill then used the credit card numbers to buy \$47,000 in goods and services.

Category 1A3 Biographical notes on individual criminals (including arrests, trials)

### 2004-05-27 Trojan Horse hacker sharing peep data theft Taiwan engineer

DHS IAIP Daily;

http://www.nytimes.com/aponline/international/AP- Taiwan- Chin

a- Cyber- Attack.html

May 27, Associated Press — Taiwan engineer accused in cyber attack.

A Taiwanese computer engineer was arrested on charges he had designed a virus- like Trojan horse that Chinese hackers found and used to attack the island's business and government systems, police said Thursday, May 27. Wang Ping- an, 30, designed "Peep," which earlier this year allowed the attackers to steal information and retain control of infected computer systems, police said. "He placed his program on popular hackers' Web sites and encouraged people to download it," said Lin Chieh- lung, an official from an Internet crime investigation task force. "He might have wanted only to show off his skills, but he should be aware what harm this could cause." If convicted on charges of vandalizing public and corporate property, he could face up to five years in prison, police said. Police said they began a probe months ago after noticing hackers had stolen confidential government data. They then discovered "Peep" was responsible for the theft of data from hundreds of Taiwanese schools, companies and government agencies. The attacks were traced back to mainland China, police said. In recent years, fears have grown that China might enforce its claim of sovereignty over self- ruled Taiwan by shutting down the island's heavily computerized society with a cyber- attack instead of a conventional invasion.

Category 1A3 Biographical notes on individual criminals (including arrests, trials)

2004-07-15 hacker New York Times Adrian Lamo hacking intrusion LexisNexis

http://www.informationweek.com/story/showArticle.jhtml?articleID=23901163

Adrian Lamo Cuts Deal With Feds

Adrian Lamo, the "Homeless Hacker," broke into the New York Times' computer network in early 2001. He surrendered to the FBI in September 2003. His modus operandi was to break into large companies networks without authorization and then offer to help them fix their security holes for free. Then he would call news reporters to boast about his exploits. In January 2004 he pled guilty in federal court to charges of computer trespass and claimed that he was remorseful about his actions. In July 2004, he was sentenced "to two years probation, with six months to be served in home detention," and also "to pay \$65,000 in restitution."

Category 1A3 Biographical notes on individual criminals (including arrests, trials)

### 2004-07-22 data theft lawsuit federal spammer spam stealing personal data fraud

NewsScan

DATA THEFT FEDERAL LAW SUIT

Federal charges have been filed against Scott Levine, the Florida spammer who ran Snipermail.com, for allegedly stealing personal data about "a great number of individuals." He is not accused of using the information for identity fraud. Prosecutors say Levine and other Snipermail employees got into the databases of Acxiom Inc. to take 8.2 gigabytes of consumer files in 2002 and 2003. Levine now stands indicted on 144 counts, including unauthorized access of a protected computer, conspiracy, access device fraud, money laundering and obstruction of justice. (AP/San Jose Mercury News 22 Jul 2004)

2004-08-05	network hacking vandalism penetration credit card system Michigan Lowes indictment
Category 1A3	Biographical notes on individual criminals (including arrests, trials)

NewsScan

NETWORK VANDALS FACE PRISON SENTENCES

Pleading guilty to attempts to hack into the national computer system of the Lowe's home improvement chain and steal credit card information, three Michigan men now face sentences of up to 25 years in prison. In the indictment, federal prosecutors had said that the men accessed the wireless network of a Lowe's store and used that connection to enter the chain's central computer system and eventually to reach computer systems in Lowe's stores across the country. Lowe's executives say the men did not gain access to the company's national database and that all customers' credit card information are secure. (San Jose Mercury News 5 Aug 2004)

Category 1A3	Biographical notes on individual criminals (including arrests, trials)
2004-08-06	hacking e-commerce fraud theft online Internet Romanian lawsuit grand jury indictment

NewsScan

INDICTMENT FOR THEFT-BY-HACKING

A Romanian and five U.S. citizens have received grand jury indictments charging them with a \$10-million scheme to steal goods by hacking into the online ordering system of computer equipment distributor Ingram Micro Inc. The Romanian, who is now in that country and not in custody, is accused of posing as a customer to place more than 2,000 orders over four years. The man is well known as a computer hacker who uses the pseudonyms "Dr. Mengele" and "Metal." After Ingram Micro blocked shipments to Romania, he allegedly recruited Americans to accept the merchandise. (AP/Los Angelese Times 6 Aug 2004)

Category 1A3 Biographical notes on individual criminals (including arrests, trials)

2004-08-12 Minnesota teenager guilty Blaster worm attack jail sentence Microsoft involvement

DHS IAIP Daily;

http://www.cnn.com/2004/TECH/internet/08/12/internet.attack.ap/index.html

August 12, Associated Press — Teen pleads guilty in Internet attack.

A Minnesota high school senior pleaded guilty Wednesday, August 11, in federal court to unleashing a variant of the "Blaster" Internet worm, which crippled more than a million computers last summer. Jeffrey Lee Parson, 19 is likely to face 18 months to three years behind bars after pleading guilty to one count of intentionally causing or attempting to cause damage to a protected computer. He also could be ordered to pay millions of dollars in restitution, Assistant U.S. Attorney Annette Hayes said. Parson had pleaded not guilty after his arrest last August, but told U.S. District Judge Marsha Pechman on Wednesday: "I downloaded the original Blaster worm, modified it and sent it back out on the Internet." Different versions of the Blaster worm, also known as the LovSan virus, crippled computer networks worldwide last summer. Parson's variant launched a distributed denial- of- service attack against a Microsoft Corp. Windows update Website as well as personal computers. The government estimates Parson's version alone inundated more than 48,000 computers. Parson was charged in Seattle, WA, last August because Microsoft is based in suburban Redmond, WA.

Category1A3Biographical notes on individual criminals (including arrests, trials)2004-09-20Sasser worm virus creator writer employment security company Germany<br/>Securepoint

NewsScan

SASSER CREATOR HIRED BY SECURITY FIRM

A German teenager accused of creating the Sasser worm that infected millions of computers around the world is being trained as a security software programmer, the company that hired him said on Friday. Eighteen-year-old Sven Jaschan has been taken on by the Securepoint computer firm based in Lüneburg, in northern Germany, and is being trained to make firewalls to stop suspect files from entering computer systems. "He has a certain know-how in this field," a company spokesman said. Jaschan has been charged with computer sabotage, data manipulation and disruption of public systems for allegedly hatching the Sasser worm. (The Age 20 Sep 2004) Rec'd from John Lamp, Deakin U.

### Category1A3Biographical notes on individual criminals (including arrests, trials)2004-11-08Nigerian scam Australia Marinellis sentencing crime 4-1-9 advance-fee fraud

prosecution trial

NewsScan; http://australianit.news.com.au/articles/0

NIGERIAN SCAMMER JAILED

The Australian mastermind of a global Internet scam was today sentenced to at least four years behind bars. Nick Marinellis pleaded guilty in the New South Wales District Court to 10 counts of fraud and one count of perverting the course of justice over the so-called Nigerian or West African scam. The ruse fleeced victims of \$5 million. Judge Barry Mahoney sentenced Marinellis to five years and three months jail with a nonparole period of four years and four months. (The Australian 8 Nov 2004)

Category 1A3	Biographical notes on individual criminals (including arrests, trials)
2004-12-21	judgement spam AOL New York CAN-SPAM insider crime

NewsScan

FORMER AOL EMPLOYEE FACES JAIL FOR HELPING SPAMMERS

Virginia software engineer Jason Smathers, formerly employed by America Online, has pleaded guilty to stealing 92 million screen names and e-mail addresses and then selling them to spammers. The spammers in turn used them to generate seven billion unsolicited e-mail messages. The 24-year-old Smathers now faces from 18 months to two years in prison and mandatory restitution of between \$200,000 and \$400,000, the estimated amount of what AOL had to spend as a result of the e-mails. Authorities said he used another employee's access code to steal the list of AOL customers in 2003 from its headquarters in Dulles, Va. He was promptly fired by the company. (AP/San Jose Mercury News 7 Feb 2005) http://www.siliconvalley.com/mld/siliconvalley/10827690.htm

### JUDGE REJECTS GUILTY PLEA IN AOL SPAM CASE

A federal judge in New York has refused to accept a guilty plea from a former AOL software engineer accused of stealing 92 million subscriber e-mail addresses and selling them to spammers. Judge Alvin Hellerstein said he was not convinced that Jason Smathers had actually committed a crime under the new "CAN-SPAM" legislation passed by Congress this fall. The technicality hinges on whether Smathers deceived anyone -- a requirement of the CAN-SPAM law. "Everybody hates spammers, there's no question about that," said Hellerstein, who told federal prosecutor David Siegal: "I'm not prepared to go ahead, Mr. Siegal. I need to be independently satisfied that a crime has been created." Prosecutors allege that Smathers sold the list to Las Vegas resident Sean Dunaway, who then resold it to spammers, netting Smathers more than \$100,000 from the deal. (Wall Street Journal 21 Dec 2004)

http://online.wsj.com/article/0,,SB110365400892306111,00.html (subscription required)

### 1A5 Criminal hacker organizations

Category 1A5 Criminal hacker organizations

### 2004-05-06 IRC viruses worms malware child pornography warez copyright infringement piracy

http://www.nytimes.com/2004/05/06/technology/circuits/06chat.html?th=&page wanted=print&position=

Seth Shiesel of the New York Times published a good review of the sociology of the IRC. He characterized the culture of the IRC in largely uncomplimentary terms. Some of the criminal activities supported by some IRC users include

\* software and movie piracy

\* child pornography

\* virus exchange

\* distributed denial of service attacks.

Law enforcement officials are very interested in the IRC but it's extremely difficult to track users, especially criminals, because of the ease with which users can switch channels.

# Category1A5Criminal hacker organizations2004-10-07cybersecurity conference globalization privacy organized crime federal research<br/>investment lacking Eugene Spafford CERIAS

DHS IAIP Daily; http://searchsecurity.techtarget.com/originalContent/0,28914 2,sid14\_gci1012829,00.html

October 07, SearchSecurity — Globalization, privacy and organized crime to drive security.

Organized crime is pouring massive amounts of resources into phishing, online extortion and other malicious activities by exploiting a U.S. weakness - - the lack of federal research and law enforcement investment in cybercrime, warned one of the nation's most influential infosecurity leaders Wednesday, October 6. "We are beginning to face well- financed, well- organized groups of professional criminals, and as far as I can tell, there's been little federal funding invested in this at all," Eugene Spafford said at the Information Security Decisions conference in Chicago. Spafford, the executive director of the Center for Education and Research in Information Assurance and Security (CERIAS), said less than \$50 million in federal funding currently is being invested in basic cybersecurity research. Attacks will come in the form of extortion, protection rackets and threats to business availability via denial- of- service attacks. Spafford said nations around the world are subsidizing hacker training programs in an effort to obtain confidential information that can benefit their businesses and citizens. Some examples include China, India, Brazil, North Korea, South Korea and Cuba.

### 1A6 Criminal hacker psychology

Category 1A6 Criminal hacker psychology

### 2004-01-14 Internet addict stereotype refuted digital divide decreasing

NewsScan

NEW STUDY REFUTES NET 'GEEK' STEREOTYPE

The typical Internet user has plenty of friends, an active social life and would rather read a good book or log on than watch TV, according to a report by UCLA's World Internet Project, which surveyed Net users and non-users in 14 countries to come up with its results. The image of Net users as socializers contradicts the stereotype of propeller-head "geeks" who spend their days (and nights) hunched over their keyboards, shunning human contact. The study did, however, reinforce some other demographic trends, including the fact that wealthier people tend to be more avid users, and that men outnumber women on the Net, although those figures vary by country, with Italy exhibiting the largest gender gap and Taiwan the smallest. Meanwhile, the digital divide — the phrase widely used to describe the disparity in Internet usage between rich and poor — appears to be narrowing around the world. Sweden, Korea and the U.S. had the largest number of low-income users. (Reuters/CNet News.com 14 Jan 2004)

Category 1A6 Criminal hacker psychology

2004-02-20 RSA security conference computer vandals social engineering hacking

NewsScan

VANDALS: BETTER AT LYING THAN AT HACKING

At a security conference last week sponsored by the security firm RSA, 10,000 computer security experts showed up — and chances were good that some of them were vandals. Ira Winkler, an expert on corporate espionage, said: "They're definitely here," in a disdainful reference to hackers whose technical skills are as meager as their personal ethics: "All you have to do is be a good liar." Some lie by stealing passwords or PIN numbers simply by looking over a user's shoulder ("shoulder surfing," it's called); others by creating spam that purposely uses misspelled words to evade spam filters. Winkler says: "They think what they're doing is special," even though it's "more difficult to learn how to protect a computer than to break into one." (San Jose Mercury News 20 Feb 2004)

Category1A6Criminal hacker psychology2004-03-04network virus worm writers fight online MyDoom Bagle Netsky

NewsScan

VIRUS WRITERS SQUABBLE ONLINE

The writers of Internet plagues MyDoom, Bagle and Netsky have ratcheted up their competition, embedding insults and threats against each other in the coding of the latest versions of their computer bugs. For example, "MyDoom.f is a thief of our idea!" and "Bagle — you are a looser!" both appear in the code of the latest Netsky worm [no one ever said worm writers were literate!]. Ken Dunham, director of malicious code at iDefense, says the spat appears to exemplify the rivalry between the authors of MyDoom and Bagle, both of which attempt to take control of infected computers, while the Netsky worm attempts to deactivate the other two. "There's a huge pool of computers that are always infected," says Dunham, who estimates that number at somewhere in the low hundreds of thousands. Virus writers "want to make sure they have complete control of those computers." Meanwhile, the new versions just keep on coming — there've been 11 versions of Bagle, seven of MyDoom and six of Netsky, which appeared only last month. "We are just seeing variation after variation," says a VP of one antivirus company. (Washington Post 4 Mar 2004)

Category 1A6 Criminal hacker psychology

#### 2004-10-21 hackers Ballmer Microsoft security

NewsScan; http://apnews.excite.com/article/20041021/D85RQQJ00.html

BALLMER SAYS HACKERS GETTING SMARTER

Microsoft chief executive Steve Ballmer says the battle against hackers has gotten harder because the hackers have gotten smarter, too. However, as a sign of the company's progress in the fight, Ballmer points to Microsoft's planned security enhancements to Windows Server 2003: "I think we've learned a lot more about security basically than anyone else in the world. That's kind of the good news and bad news, being the position we've been in with our kind of market share." (AP 21 Oct 2004)

### 1B1 Adult pornography

Category 1B1 Adult pornography

### 2004-01-10 pornography DVD HD-DVD Blu-ray high-resolution

NewsScan; http://www.washingtonpost.com/wp-dyn/articles/A62546-2005Jan10.html?nav=headlines

#### PORN DRIVES DVD TECHNOLOGY

Just as it has with other home entertainment technologies, pornography is proving a driving force in the future of highdefinition DVDs. The multi-billion-dollar industry releases about 11,000 DVD titles a year, giving it a strong position in the debate over which technical standard -- Blu-ray or HD-DVD -- will dominate in next-generation DVDs. Analysts say currently, the smaller outfits are leaning toward HD-DVD because of its lower cost, while larger operations like Blu-ray's bigger storage capacity, which could be used for "creative expression" -- like giving viewers a choice of camera angles. Hollywood is also lining up on both sides of the battle, with Fox and Disney declaring their preference for Blu-ray and Warner Home Video siding with HD-DVD. But for now, everyone's kind of waiting around to see which format takes the lead. "We're kind of riding it out a little further to see where the trend goes," says an executive with leading porn producer Wicked Pictures. (Reuters/Washington Post 10 Jan 2004)

### Category 1B1 Adult pornography

2004-02-08 pornography porn digital piracy unworried intellectual property rights copyright

NewsScan

### PORN INDUSTRY VIEWS PIRACY AS 'DIRECT MARKETING'

The pornography industry takes a very different view of digital piracy than their counterparts in Hollywood and the music business — they're all in favor of it. "It's direct marketing at its finest," says Randy Nicolau, president of Playboy.com, who doesn't mind one bit that his magazine's pictures appear on thousands of other Web sites. When asked whether he thinks the entertainment industry is on the wrong track with their prosecution of online freeloaders, Nicolau says, "I haven't spent much time thinking about it. It's like asking Henry Ford, 'What were the buggy-whip guys doing wrong?'" And while the folks peddling porn may have a live-and-let-live attitude when their content gets ripped off, they show a different face when someone else is making money off of it. "We haven't gone after Joe Citizen who's sharing something he printed off something from the Hustler Web site with another guy," says a lawyer who represents Hustler on copyright issues — but he does send out about 20 letters a week to fee-based Web sites who are charging for his client's content. Meanwhile, another group, Titan Media, tracks down copyright violators and then offers them amnesty if they will become subscribers, an approach that may work for other content owners, says Wendy Seltzer, a staff attorney for the Electronic Frontier Foundation who calls it "a much more sensible approach" than the music industry's litigation strategy. "People always want this stuff. Seeing some of it just whets their appetite for more. Once they get through what's available for free, they'll move into the paid services." (New York Times 8 Feb 2004)

Category 1B1 Adult pornography

### 2004-03-09 pornogrpahy porn industry business model innovative profitable Internet

NewsScan

PORN: TRASH INTO CASH

It could be called high-tech's dirty little secret. Some of the Web's most innovative and profitable entrepreneurs are online pornographers, who for more than a decade have been among the first to exploit such new technology as video-streaming, feebased subscriptions, pop-up ads, and electronic billing. In fact, porn is one of the most profitable online industries, and it's venturing into such new fields as wireless services and digital-rights management. One Internet porn entrepreneur started her business by posting to the Internet some photos she'd retrieved from a trash bin: "Technology turned trash into cash. That's a lesson other industries can learn." (USA Today 9 Mar 2004)

### Category 1B1Adult pornography2004-05-14australia mobile porn Daryl Williams telecommunications watchdog adult content

NewsScan

AUSTRALIAN CRACKDOWN ON MOBILE PORN

Risqué adult material will no longer be accessible to children using mobile phones in Australia, under new regulatory changes. Australian Communications Minister Daryl Williams said he had ordered the telecommunications watchdog to put in place new measures to protect hi-tech mobile phone users from offensive content. As part of the new measures, the Australian Communication Authority (ACA) will regulate access to content provided on new premium mobile phone services. "These new measures will help make access to the Internet and mobile communications services safer and more enjoyable for all Australians, particularly children," says Williams. "These controls will restrict access by children to adult content." (The Australian 14 May 2004) rec'd from John Lamp, Deakin University

Category 1B1 Adult pornography

2004-05-25 porn offshore australian users phone bills dial-up services overseas lines providers

NewsScan

PORN DUMPERS MOVE OFFSHORE

Some Australian Internet users are getting huge bills for phone calls to exotic overseas locations, as providers of Internet pornography move Internet dialing services offshore. Dial-up Internet users are disconnected from their Internet service provider and then reconnected without their knowledge to a premium overseas line. Charges are then split between the telcos and the content provider. Many embarrassed users claim to have been "dumped" — i.e., connected to a premium-rate call without being fully informed of the cost of the call. (The Australian 25 May 2004) Rec'd from John Lamp, Deakin U

Category 1B1 Adult pornography

2004-06-29 online pornography law unconstitutional Supreme Court wary First Amendment

NewsScan

SUPREME COURT WARY OF ONLINE PORNOGRAPHY LAW

The Supreme Court has ruled in a 5-4 decision that a law meant to protect children from exposure to online pornography is probably an unconstitutional restriction on free speech guaranties of the Constitution's First Amendment. The law, which passed in 1998 and was signed by then-President Clinton, is now backed by the Bush administration. Known as the Child Online Protection Act, the law would have authorized fines up to \$50,000 for the crime of placing material that is "harmful to minors" within the easy reach of children on the Internet. The majority opinion, written by Justice Anthony M. Kennedy, said that "there is a potential for extraordinary harm and a serious chill upon protected speech" if the law were to take effect. The case has been sent back to a lower

court for a trial that would allow a discussion of what technology, if any, might allow children to be shielded from online pornography but at the same time would allow adults to see and buy any material that is not illegal. (AP/Washington Post 29 Jun 2004)

Category 1B1 Adult pornography

#### 2004-08-17 pornography study Australia sexuality children protection hard core

NewsScan

NET-PORN IS GOOD FOR YOU, SAY ACADEMICS

Pornography is good for people, says the academic leading an Australian taxpayer-funded study of the subject. Alan McKee and his colleagues Catharine Lumby and Kath Albury are conducting the Understanding Pornography in Australia study. The Labor party is considering forcing Internet service providers to filter hardcore porn in order to protect children using home computers. McKee says: "The surprising finding was that pornography is actually good for you in many ways. When you look at people who are using it in everyday life, over 90% report it has had a very positive effect" because it had taught them to be "more relaxed about their sexuality," made them think about another person's pleasure, and made them less judgmental about body shapes. (The Australian 17 Aug 2004) Rec'd from John Lamp, Deakin U.

Category	1B1	Adult pornography
----------	-----	-------------------

2004-08-25 Geman police swap pornography e-mail law enforcement

NewsScan

GERMAN POLICE ACCUSED OF E-MAIL PORN-SWAPPING

Two dozen German police officers suspected of using office computers to exchange pornographic messages. These activities were discovered by a maintenance technician who then reported them to his superiors. The police officers being investigated face possible disciplinary sanctions and could he brought before a judge. (The Arg 25 Aug 2004) Recid from L Lamp

be brought before a judge. (The Age 25 Aug 2004) Rec'd from J. Lamp

Category 1B1 Adult pornography

#### 2004-10-25 pornography wireless profit bandwidth

NewsScan;

http://www.reuters.com/newsArticle.jhtml;jsessionid=TPZD2EKVY5JQSCRBAE OCFEY?type=technologyNews&storyID=6600488

#### ADULT CONTENT TO BOOST WIRELESS WEB SERVICES

Analysts say porn purveyors will do the same thing for the wireless sector that they did for the fixed-line Internet, fueling major growth while raking in the bucks. In the U.S., consumers will shell out some \$90 million for adult entertainment in four years' time, according to a report by Yankee Group, which estimates that excluding portals of U.S.- based wireless operators, half of all wireless data traffic consists of pornography. Meanwhile, the only thing holding back the U.S. carriers is the worry over a backlash if adult content falls into the hands of children: "Fear is trumping greed for the moment, but the two can work together if carriers can develop a solid mechanism for protecting minors and safely profit from the opportunity," says Yankee. (Reuters 25 Oct 2004)

#### Category 1B1 Adult pornography

#### 2004-11-22 pornography Google copyright images piracy search engine lawsuit

NewsScan; http://www.wsj.com/

ADULT-ENTERTAINMENT GROUP SUES GOOGLE

In a federal lawsuit filed against Google, the adult-entertainment firm Perfect 10 Inc. is charging that Google's search engine has been displaying copyrighted images from Perfect 10's magazine and Web site, along with passwords to its subscription Web site, in response to user queries. The company says that Google's computers retrieve the passwords and images (mainly photos of female models) not from Perfect 10's own site but from other sites that have pirated them; charging that it would be "virtually impossible" for consumers to locate the stolen content if Google didn't direct them to it, its complaint accuses Google of "putting them on their servers knowing in most cases these pictures are unauthorized." Google has not yet responded to the complaint. (Wall Street Journal 22 Nov 2004)

# 1B2 Child pornography

Category 1B2 Child pornography

#### Child pornography John B Martin sex offender internet

2004-01-05 NewsBits;

http://www.zwire.com/site/news.cfm?BRD=1302&dept\_id=181981&newsid=107 38256&PAG=461&rfi=9

Supreme Court upholds convictions for child pornography

John B. Martin, 64, of Belle Fourche, South Dakota, was convicted in 2002 of having child pornography on his office and home computers; he claimed that his three-year project of collecting pornography was an attempt to provide evidence for new antiporn laws. Records showed no attempts to contact government or law enforcement on this subject. He was sentenced to 90 days in local prisons in lieu of several years in federal prison. In his appeal against this sentence, his attorneys argued that the child pornography laws were unconstitutional because their overly-broad language could forbid ownership of digitally-created or modified images that did not in fact involve real children. In a decision on his appeal, the Supreme Court of the United States (SCOTUS) ruled unanimously that "the laws did not violate the U.S. Constitution, did not improperly restrict free speech and gave Martin adequate notice of what activities were illegal."

Category 1B2 Child pornography

2004-01-05 child pornography Alfred Wayne Velasquez sexual assault internet

NewsBits;

http://www.wfaa.com/localnews/stories/010104dnmetvelasquez.4b50f.html

Fort Worth man makes plea deal in sex case

A 36-year-old Fort Worth man suspected of having sex with underage girls he met through the Internet has struck a deal with Tarrant County prosecutors that includes an eight-year prison sentence. Alfred Wayne Velasquez pleaded guilty last month to sexual assault of a child for having sex with a 14-year-old Arlington girl in September 2001 at her house while her parentsere away. Mr. Velasquez has been indicted on similar charges in Johnson and Collin counties. Plea agreements are likely in those jurisdictions, but nothing has been finalized, officials said. Mr. Velasquez was being held in the Tarrant County jail in lieu of \$225,000 bail.

Category 1B2 Child pornography

#### Child pornography Roger Jacobs internet prostitution

2004-01-05 NewsBits;

http://rockymountainnews.com/drmn/local/article/0,1299,DRMN\_15\_2547407,0 0.html

Appeals court rules child-porn term unjustified

The state Court of Appeals vacated the sentence of a man convicted in an Internet child-porn case, ruling his term of 25 years to life was not warranted. The court said Wednesday there wasn't enough evidence to justify an indeterminate sentence for Roger Jacobs, convicted of two counts of soliciting for child prostitution. Jacobs was convicted after a California detective set up an Internet site offering "very young, very attractive escorts," and Jacobs, who lived in Westminster, responded. The detective sent Jacobs a picture of a girl and told Jacobs she was 12 years old. Jacobs sent the detective a picture of himself and the type of girl with whom he would like to have sex.

Category1B2Child pornography2004-01-13child sex case nude photogragpy pornography Stephen Wilson

NewsBits;

http://www.fayettevillenc.com/story.php?Template=local&Story=6115863

Suspect in child-sex case arrested on new charges

A Fayetteville, NC man faces a second round of charges that he possessed nude photographs of girls as young as 12. Stephen Wilson, 28, was charged in early January with first-degree sexual exploitation of a minor. According to an arrest warrant, girls posed for Wilson "in a sexual manner" as he photographed them with a digital camera. Sheriff's Detective J. Stallings said in a magistrate's document that Wilson downloaded the photos onto his computer. Stallings said a forensic pediatrician examined the images and estimated the unknown girls to be 12 or 13. "Mr. Wilson also admitted to downloading pictures from the Internet of teenage girls for his own curiosity," Stallings said.

Category 1B2 Child pornography

#### 2004-01-16 child pornography pedophilia

NewsBits; http://wildcat.arizona.edu/papers/97/75/01\_1.html

Student charged in child porn case

A UA student has pled guilty to charges of downloading child pornography and sharing the material over the Internet while he lived in a campus residence hall last fall, officials said. Donilo Phillip Colich, 20, was charged with one count of attempted sexual exploitation of a minor under 15, a class 2 felony, according to UAPD Sgt. Eugene Mejia. Colich, originally indicted on 11 counts, received 10 years of probation last week, which includes no access to children and the Internet. He will also have to register as a sex offender, said Assistant County attorney Kathleen Mayer. On Nov. 12, 2002, an unknown person from Switzerland notified the UA webmaster that Colich had been using the KaZaA file-sharing program to download child pornography in his room in the Manzanita-Mohave Residence Hall, 1010 NewsBits; . Park Ave. The webmaster notified the computer management division on campus, which was able to trace the files back to an IP address that corresponded to Colich's computer.

Category 1B2 Child pornography

2004-01-20 internet pornography probe charges child

NewsScan

PORN PROBE

Officers investigating child porn have identified nearly 250 residents across the region who have accessed indecent websites. The figures are being discussed by Hampshire Police Authority at a meeting today. Panel members will be told that Operation Danforth is still a major commitment to the force, with 238 residents of Hampshire and the Isle of Wight identified as accessing websites containing indecent images of children. There's also a warning that on-line storage, encryption and file sharing are making the police's investigations more difficult.

Category 1B2 Child pornography

#### 2004-01-21 child pornography sentence Clifford James Robinson

NewsBits; http://www.nzherald.co.nz/latestnewsstory.cfm?storyID=3544951

Jail term for child porn trader pleases investigators

Child pornography investigators are pleased with the jail term handed down to a Christchurch New Zealand, man yesterday for copying and possessing images of adults sexually abusing children, incest and bestiality. The Internal Affairs Department polices illicit publications, including images traded on the internet. Clifford James Robinsin, 38, was jailed in January for seven months for trading a three-minute movie of a baby girl being sexually abused and 22 other charges relating to objectionable images, transcripts, and movies.

Category 1B2 Child pornography

2004-01-21 Christopher Wade Ooms child pornography plead

NewsBits;

http://www.swtimes.com/archive/2004/January/21/news/child\_porn.html

Van Buren Man Gets Probation In Child Porn Case

A Van Buren man accused of using his neighbor's computer to surf the Internet in search of child pornography has been sentenced to probation. Christopher Wade Ooms, 20, pleaded no contest Tuesday to one count of pandering or possessing visual or print medium depicting sexually explicit conduct involving a child. Ooms was arrested in April after a neighbor contacted police and said that she found sexually explicit material on her computer after Ooms used it.

Category 1B2 Child pornography

#### 2004-01-22 child pornography distribution

NewsBits; http://www.southbendtribune.com/stories/2004/01/15/local.20040115-sbt-MARS-A2-Prosecutor\_s\_staff\_g.sto

Indiana Prosecutor's staff goes after child pornography on Net

An undercover investigation by the St. Joseph County, IN prosecutor's office has identified 26 people around the world suspected of possessing or distributing child pornography on the Internet. The monthlong investigation resulted in the seizure of more than 10,000 images and movies portraying child pornography, officials reported. During the operation, Mitch Kajzer, an investigator in the prosecutor's office, posed on the Internet as someone who wanted to trade child pornography files, said Prosecutor Michael Dvorak. In just one month, more than 100 people approached Kajzer wanting to download child pornography and Kajzer traded with 39 of them. Twenty-six of those people now face criminal charges such as child exploitation, possession of child pornography and distribution of child pornography.

Category 1B2 Child pornography

#### 2004-01-30 Child Pornography county sherrif Gary Penrod Vertican

NewsBits;

http://www.dailybulletin.com/Stories/0,1413,203%7E21481%7E1921248,00.html

Suit against sheriff cost county \$50,000

The federal lawsuit filed against San Bernardino County Sheriff Gary Penrod and two others cost taxpayers \$50,000 to defend only to be dropped by the plaintiff under a settlement before it went to trial. Gary Vertican's \$60 million lawsuit filed in U.S. District Court in Riverside against Penrod, sheriff's Detective Michael DiMatteo and Probation Officer Melinda Carpenter on Feb. 24 disintegrated for lack of evidence, attorneys for both sides said Tuesday. In the lawsuit, the former Twin Peaks resident accused DiMatteo of planting evidence of child pornography on computer disks seized with a warrant from Vertican's home in February 2002.

Category 1B2 Child pornography

#### 2004-01-30 Kelly child pornography trial evidence search seizure

NewsBits; http://www.theledger.com/apps/pbcs.dll/article?AID=/20040130/NEWS/401300 393/

Judge to Rule On Evidence in Illinois Child Porn Case

Lawyers for R&B star R. Kelly, who is facing child pornography charges in Polk County and Chicago, have asked a judge to throw out key evidence in the singer's local case, arguing it was seized during an illegal search. In a motion filed last week, Bartow lawyer Ron Toward argued that prosecutors should not be allowed to use the evidence, including a digital camera that investigators said contained 12 nude pictures of an underage girl. The evidence was seized during what Toward described as an illegal search of one of two houses Kelly was renting in the Ridgewood Lakes subdivision near Davenport in June 2002.

Category 1B2	Child pornography
2004-01-30	child pornography Boy Scout volunteer teacher Maxwell

NewsBits

NJ Substitute Teacher Accused Of Possessing Child Porn

A 53-year-old substitute teacher and Boy Scout volunteer was arrested and charged with possession of child pornography, federal authorities said. John Maxwell of Clifton was released Thursday after posting \$100,000 in unsecured bonds, said Brett Dreyer, a spokesman for the U.S. Immigration and Customs Enforcement agency. The criminal complaint, filed in U.S. District Court in Newark, alleged that Maxwell downloaded more than 100 pornographic images onto his personal computer from the Internet. Federal authorities seized the computer and other evidence during a search of Maxwell's home in January, authorities said in a statement.

Category 1	B2 Child <sub>I</sub>	oornography		
		_		

#### 2004-02-27 child pornography Europe raids arrests Internet

NewsScan

CHILD PORN RAIDS IN TEN EUROPEAN COUNTRIES

Interpol, the European Union police agency, says that coordinated police raids in 10 countries have broken a number of Internet child pornography networks and arrested people in more than 40 locations. The main focus of the raids were in Wiesbaden, Germany, but other countries where raids took place were Australia, Belgium, Canada, the Netherlands, Norway, Peru, Spain, Sweden and Britain. (Los Angeles Times 27 Feb 2004)

Category	1B2	Child pornography
----------	-----	-------------------

#### 2004-09-20 child pornography Switzerland police arrest

NewsScan

#### SWISS POLICE ARREST TEN OVER CHILD PORN

Swiss police have arrested 10 people and carried out about 400 searches in a massive nationwide operation against international child pornography networks operating in Switzerland. Swiss Federal Police say they seized large quantities of material including computers during the ten-day swoop,

which was prompted by investigations into child porn websites in the United States. Another 120 countries are concerned by the probe, which follows on from a similar international operation in 2002. (The Age 20 Sep 2004) Rec'd from J. Lamp

Category 1B2 Child pornography

#### 2004-09-30 child pornography Australia international global warrants credit cards

NewsScan; http://theage.com.au/articles/2004/09/29/1096401645228.html

CHILD INTERNET PORN RING SMASHED

Australian police and U.S. FBI agents have smashed a global Internet child pornography ring, with hundreds of search warrants issued on properties throughout Australia. Though it's often difficult to catch Internet child porn users, some of the perpetrators used their own credit cards to gain access to illegal images.

### 1B3 Pedophilia, kidnapping, Netadoption fraud

Category 1B3 Pedophilia, kidnapping, Net-adoption fraud

#### 2004-01-05 child exploitation sexual contact pedophilia David Gipson Jr.

NewsBits; http://www.cincypost.com/2004/01/03/briefs01-03-2004.html

Man held on sex charge

A North College Hill man has been arrested and charged with unlawful sexual contact after authorities said he tried to solicit sex from a 14-year-old female on the Internet. The minor was in fact a detective with the Regional Electronic and Computer Investigations, which is made up of deputies, officers and detectives from the Cincinnati police department and Hamilton County Sheriff's Department. David Gipson Jr., 32, was arrested in Sycamore Township on Monday and charged with one count of attempted unlawful sexual contact with a minor and one count of importuning. Authorities arrested Gipson at the location he designated to meet the girl.

Category 1B3	Pedophilia, kidnapping, Net-adoption fraud
2004-01-13	underage sexual assault internet pedophile Nicholas Ardent cyber sting exploited child

NewsBits;

http://www.greenbaypressgazette.com/news/archive/local\_14141664.shtml

Green Bay, Wisconsin Area man charged in child-sex sting

A 22-year-old De Pere man was arrested Saturday after he allegedly arranged to have sex with 10- and 12-year- old girls while their father watched. However, hat father turned out to be special agent Eric Szatkowski of the state Department of Justice Division of Criminal Investigation. Nicholas Arendt now faces two counts of attempted sexual assault of a child under 13. Szatkowski zeroed in on Arendt after a complaint was filed with the cyber-tip line of the National Center for Missing and Exploited Children. According to the criminal complaint filed Monday in Brown County Circuit Court, Szatkowski first posed as the father of two young girls, ages 10 and 12, in an Internet chat room and agreed to bring his children to Arendt's Morning Glory Road apartment for sex.

Category 1B3 Pedophilia, kidnapping, Net-adoption fraud

2004-01-14 pedophile internet stalking police investigation prosecution sentencing

NewsBits; http://www.smh.com.au/articles/2004/01/15/1073877933063.html

University student first to be sentenced over internet porn

An Australian university graduate is facing jail under tough new Queensland laws aimed at catching pedophiles preying on children in internet chat rooms. Matthew William Ross Kennings will be the first person sentenced under the laws next month after pleading guilty in the District Court in Brisbane yesterday. The 26-year-old refugee centre volunteer was charged in July last year with intending to procure a person he believed to be under 16 years old to engage in a sexual act. The new laws were introduced two months beforehand, with police and the state's Crime and Misconduct Commission setting up a joint operation to target offenders. Kennings was caught after making contact with one of the officers who was posing as a 13-year-old girl using the name BeckyBoo13 in internet chatroom MSN Whisper.

#### Category 1B3 Pedophilia, kidnapping, Net-adoption fraud

#### 2004-01-14 net prowler laws legislation Jeff Denham

NewsBits; http://www.modbee.com/local/story/8003223p-8870893c.html

California Legislation to fight Net prowlers halted

An effort by Sen. Jef f Denham, R-Merced, to better nab Internet child-sex prowlers died in a committee hearing Tuesday when not enough senators showed up to vote. California Senate Bill 882 failed on a 2-0 vote in the Senate Public Safety Committee. The bill needed a majority, or four votes, to move out of the six- member panel. Denham expressed disappointment that his bill died because of procedural rules. A similar effort passed out of the same committee two years ago but later stalled.

Category 1B3	Pedophilia, kidnapping, Net-adoption fraud
2004-01-20	child molester pedophilia internet

NewsScan

CONVICTED CHILD MOLESTER ACCUSED OF SECOND CRIME

A former Fort Hood soldier has been convicted in Montague for stalking a 14 year old Bowie girl after meeting her on the Internet. While out on bond on that charge, he was arrested for allegedly trying to solicit sex with a 15 year old girl in Bastrop county. That girl turned out to be an attorney general cyber crime unit investigator.

Category 1B3 Pedophilia, kidnapping, Net-adoption fraud

2004-01-21 pedophile sting Gudzyk

NewsBits; http://www.mcall.com/news/local/allb3\_1cyberpervjan10,0,4631594,print.story

Pennsylvania man busted in online pedophile sting, police say

A 49-year-old Carbon County, PA man who used the Internet to arrange a sexual tryst with what he believed was 12-year-old girl sped off from a store when he saw he was about to be arrested, and was stopped only after a detective fired bullets into the car, according to court documents. No one was injured. Ernest R. Gudzyk of 3 Spring Valley Farms, Weatherly, was arrested when he drove up to a King of Prussia grocery store where he had arranged to meet the girl, actually a Montgomery County detective posing as a child to catch online pedophiles, the documents said.

Category1B3Pedophilia, kidnapping, Net-adoption fraud2004-01-21sex abuse internet solicitation pedophilia child pornography John McPartland

NewsBits; http://www.katu.com/news/story.asp?ID=63779

Oregon teacher investigated on sex abuse charges

A teacher and coach at a middle schol in Gresham, OR is on administrative leave after his arrest by the FBI and local police on charges of trying to use the Internet to solicit a boy for sex. The "boy" was actually an undercover federal agent. Agents arrested 42-year-old John McPartland Friday at his apartment. He is a math teacher and basketball coach at Clear Creek Middle School. The investigation was done by the FBI's Innocent Images Task Force, which focuses on child pornography and people who use the Internet to prey on children. District plans sexual predator training.

2004-01-21	internet child stalking sex offender pedophilia
Category 1B3	Pedophilia, kidnapping, Net-adoption fraud

NewsBits; http://www.thestate.com/mld/thestate/news/local/7762250.htm

SC Attorney General pushes to outlaw Internet child stalking

A bill that would make enticing children using the Internet illegal in South Carolina was unanimously approved Wednesday by a SC House subcommittee. If passed by legislators, it would be the first law in the state barring adults from luring children to have sex or commit crimes. The bill makes it easier to prosecute these crimes by expanding the state grand jury's authority to investigate them, state Attorney General Henry McMaster said. Sexual cybercrimes often cross state lines because the Internet enables predators to contact children in practically any part of the world.

Category	1B3	Pedophilia,	kidnapping,	Net-adoption fraud
----------	-----	-------------	-------------	--------------------

2004-01-23 sex offender registration California

NewsBits;

http://www.mercurynews.com/mld/mercurynews/news/local/7778004.htm

Sex offender data posting gains support

Prospects for Californians to get better information about registered sex offenders living among them are the strongest they have ever been, after sharp scrutiny of the state's Megan's Law. After years of failed efforts, state leaders say they are optimistic about passing legislation to put the names, photographs and exact addresses of high-risk sex offenders on the Internet. A Mercury News investigation last month showed that most states already provide that information online, while California clings to a system that is one of the most restrictive and error-riddled in the country.

### Category 1B3 Pedophilia, kidnapping, Net-adoption fraud

2004-01-30 sexual abusers sentencing Salazar pedophilia criminal record seduction Internet

NewsBits; http://www.tecrime.com/llartL06.htm

Sexual abusers of children often get deals, no convictions

Manny Garcia and Jason Grotto wrote a report for the Miami Herald about the variable prosecutions of men caught seducing minors into sexual relations. In one case, 20-year-old Alan Salazar was arrested in Houston after arranging for a 14-year-old Dania Beach, FL teenager to fly to Texas. The perpetrator "pleaded no contest to interfering with the custody of a minor, [but] a Broward County judge withheld adjudication, meaning Salazar can say he has never been convicted of a crime." According to research by the newspaper staff, most of the Internet seduction cases end up without convictions even though the criminals plead guilty or no contest; about 80% of the child pornographers arrested in the state have their convictions erased from their criminal records. "Investigators blame the Florida Criminal Punishment Code, which scores some Internet sex crimes no worse than writing a bad check at the grocery store." Defense attorneys claim that their clients did not know that their victims were minor; some accuse police of entrapment when the officers impersonate children online.

Category 1B3 Pedophilia, kidnapping, Net-adoption fraud

#### 2004-06-09 Internet chat room pedophiles monitor joint efforts

NewsScan

PATROLLING INTERNET CHAT ROOMS

Law enforcement agencies in Britain, Australia, Canada and the U.S. are planning joint patrols of Internet chat rooms in search of pedophiles. Their hope is to establish a "24/7 police presence on the Internet." Jim Gamble of the UK's National Crime Squad says: "We're looking to put a police presence on the Internet in an overt way that reassures people." The four countries plan to develop a "simple visible logo" to indicate police presence in a chat room, and Gamble explains: "I don't think we're talking about devoting massive numbers to this... People feel safer when police are present, it's as simple as that. There is no Big Brother initiative here, this is about reassurance through visibility." (AP/Los Angeles Times 9 Jun 2004)

Category 1B3 Pedophilia, kidnapping, Net-adoption fraud

2004-07-19 Web alert system Amber child abduction kidnapping monitor thwart

NewsScan

AMBER ALERT COMES TO THE WEB

The nation's Amber Alert system will be connected to the Web starting today, making it easier for that system to thwart child abductions by transmitting messages about child abductions. An executive of the company that designed the Amber Alert portal says: "The tag line on all this is, 'We'll all be looking for you.' This unbelievable technology is going to make that possible." Speed is considered vital in recovering an abducted child. The Justice Department estimates that three of every four victims are killed within three hours of being taken. (USA Today 19 Jul 2004)

### 1B4 Stalking & harassment

Category 1B4 Stalking & harassment

#### Internet stalker victim compensated Docusearch private information revelation

2004-03-10 NewsScan

MOTHER OF INTERNET STALKER'S VICTIM GETS \$85,000 FROM DOCUSEARCH

Docusearch, an Internet information broker which provided information used to stalk and murder a young woman with whom he was obsessed, has agreed to pay \$85,000 to the victim's mother. Although Docusearch insists that none of the information it provided was private, the victim's mother says the company invaded her daughter's privacy and broke other laws in helping the obsessed stalker to find her. The woman's lawyer warned that information brokers such as Docusearch "will have to pay attention to whom they are providing people's private information," and he accused Docusearch of having "laid a red carpet" for the stalker which led him to the victim's place of employment. (AP/USA Today 10 Mar 2004)

Category 1B4	Stalking & harassment
2004-04-26	Internet stalking lawsuit annoyance abuse threat lawsuit prosecution

NewsScan

'FACELESS ENTITY' SAYS HE ISN'T A STALKER

In a South Carolina federal courtroom, a 38-year-old man named Robert James Murphy has pleaded innocent of Internet stalking charges and now remains free on \$50,000 bond. Murphy was charged with 26 counts of using his computer "to annoy, abuse, threaten and harass" a Seattle woman who had never seen him until the day of his court appearance. The woman says: "He didn't give me any eye contact. He has been a faceless entity to me. I wanted to see him, and I wanted him to know that I was looking at him." If convicted, Murphy faces as many as 52 years in prison. He is accused of sending obscene messages and pictures to the woman and her co-workers beginning in 1998 — tracking her from his computer as she moved from state to state and job to job. For several years she had been simply deleting and ignoring the man's messages, but then began saving them as evidence and eventually approaching the police. (AP/USA Today)

Category 1B4 Stalking & harassment

#### 2004-11-02 Internet stalking South Carolina sentencing probation commuty service restitution email fax authenticity forgery

NewsScan; http://apnews.excite.com/article/20041102/D863O0TO0.html

INTERNET STALKER IN ANOTHER 'BAD PATCH' OF HIS LIFE

A South Carolina man has been sentenced to five years of probation, 500 hours of community service, and more than \$12,000 in restitution for breaking a federal Internet stalking law by sending dozens of e-mails and faxes to a woman who broke up with him more than a decade ago. He also made it appear that the woman was sending pornographic material to her colleagues. The man now acknowledges that he was "stupid, hurtful and just plain wrong" to torment the woman, and says: "I was going through a bad patch in my life. I want to take my lumps and get on with life." He could have faced two years in prison and a fine of \$250,000, but prosecutors agreed to recommend a sentence of three to five years on probation. (AP 2 Nov 2004)

## 1B5 Gambling

Category 1B5	Gambling
2004-03-01	Internet online gambling gaming security dishonest manipulation prevention software

NewsScan

**KEEPING ONLINE GAMES HONEST** 

IT GlobalSecure sells software that prevents network vandals and dishonest players from manipulating online gambling. The company's chief executive says: "If you look online, there are whole Web sites either complaining about cheating or sharing ways to cheat. We've had people who are even just playing gin rummy online saying, 'We think we're being cheated, but we don't know what to do.'" The firm's software is based on encryption technology that can be applied to any network gaming system to validate the randomness of events in games of chance, verify player identities and create audits of each game. (Washington Post 1 Mar 2004)

Category 1B5	Gambling
2004-05-31	offshore online gambling prosecution domestic support services international law first amendment rights litigation

http://www.nytimes.com/2004/05/31/technology/31 gambling.html?th=&pagewanted=print&position=

In early April 2004, United States Marshals seized \$3.2M in advertising fees paid to the Discovery Communications Corporation for TV ads promoting the online gambling service ParadisePoker.com. Online gambling is illegal in the United States, but offshore gambling facilities cannot be attacked because the countries where they reside do not consider them illegal. Under international law, the doctrine of dual criminality requires equivalent crime laws in order to extradite people accused of a crime in one jurisdiction from the jurisdiction where they reside. Therefore, federal law enforcement authorities are cracking down on online gambling by attacking American companies who provide services to those offshore organizations. Critics of the new campaign argue that US law is inconsistent with respect to online gambling because not all states make it illegal. In addition, some analysts raised First Amendment rights arguments. Others complain that seizing foreign funds is a violation of international law.

### **1B6** Auctions

Category 1B6 Auctions

#### 2004-05-09 eBay guarantee auctions marketing future prediction

http://www.nytimes.com/2004/05/09/business/yourmoney/09digi.html?th=&pag ewanted=print&position=

Randall Stross wrote about eBay's lack of guarantees. He observed that transactions are changing from low-cost, used products being exchanged under auction to high-cost, new products sold under a fixed price. He predicted that the company would eventually have to start providing moneyback guarantees to remain competitive.

#### Category 1B6 Auctions

#### 2004-11-07 eBay price inflation New York crime shills fraud bidding overpayments

NewsScan; http://www.washingtonpost.com/wp-dyn/articles/A32944-2004Nov7.html

BIDDING UP PRICES ON ONLINE AUCTIONS

Eight eBay sellers who bid up products online to inflate their prices have been ordered by the New York Attorney General's office to pay almost \$90,000 in restitution and fines. More than 120 people will receive money from the settlement of the three cases. One man will receive a check for \$3,089 after overpaying for a 1999 Jeep Cherokee sport-utility vehicle he bought from an eBay seller in 2002. (Washington Post 7 Nov 2004)

Category 1B6 Auctions

#### 2004-11-17 eBay Virgin Mary cheese sandwich auction joke

NewsScan; http://theage.com.au/articles/2004/11/16/1100574471142.html

BIDS FOR VIRGIN MARY CHEESE SANDWICH CANCELED

The folks at eBay were no believers in this cheesy miracle: half of a 10-year-old grilled cheese sandwich whose owner claimed it bore the image of the Virgin Mary. Diana Duyser put the sandwich up for sale last week, drawing bids as high as \$22,000 before eBay pulled the item on Sunday night. The page was viewed nearly 100,000 times before being taken down. An e-mail Duyser received from eBay said the sandwich broke its policy, which "does not allow listings that are intended as jokes." (The Age 17 Nov 2004)

### **1B7** Hate groups, speech

Category 1B7 Hate groups, speech

#### e-mail racism hate Australia law enforcement police controversy

2004-03-17 NewsScan

AUSTRALIAN POLICE IN RACIST E-MAIL CONTROVERSY

The New South Wales ombudsman will help police decide how to discipline an officer who sent a racist email to his colleagues. The contents of the email, found in the in-boxes of offices in four regional stations including Broken Hill and Dubbo, were described as filthy and disgusting by Deputy Commissioner David Madden at the time of its discovery. Thirty-five officers received the e-mail but the message is thought to have originated from a single source, who has been identified as an officer from Bourke in central northern NSW. The discovery of the e-mail came just two weeks after an alleged riot in the inner-Sydney suburb of Redfern, in which 36 officers were injured. The riot was in response to the death of an Aboriginal teenager. (The Australian 17 Mar 2004)

Category 1B7 Hate groups, speech	
----------------------------------	--

### 2004-04-28 hate group Internet Web counter-terrorism homeland security freedom of speech first amendment violence

NewsScan

HATE GROUPS ON THE INTERNET

Since the recent conviction in Illinois of a white supremacist who tried to have a judge murdered, the FBI has increased its monitoring of Web sites operated by hate groups. Richard K. Ruminski, the FBI official in charge of counter-terrorism investigations in Chicago, has made it clear that the agency won't tolerate anyone crossing the line from protected free speech to advocating violence. Ruminski says of one site: "It concerns us to the point where we're going to see what legal actions can be taken in order to maybe legally take that Web site down." (AP/Los Angeles Times 28 Apr 2004)

Category 1B7	Hate groups, speech
2004-06-17	hate sites fighting conference Paris free speech censorship
NewsScan	

HATE SITES

An international conference in Paris has been exploring ways to fight anti-Semitic, racist and xenophobic propaganda on the Internet. "Our responsibility is to underline that by its own characteristics -- notably, immediacy and anonymity -- the Internet has seduced the networks of

intolerance," French Foreign Minister Michel Barnier told the conference attendees. However, U.S. Asst. Attorney General Dan Bryant urged caution in taking actions that would violate rights of free speech, and suggested that the appropriate test is always whether a particular Web site is or is not

engaged in criminal activity: "We believe that government efforts to regulate bias-motivated speech on the Internet are fundamentally mistaken. At the same time, however, the United States has not stood and will not stand idly by, when individuals cross the line from protected speech to criminal conduct." (AP/San Jose Mercury News 16 Jun 2004)

### **1B9** Non-virus hoaxes, urban myths

Category 1B9 Non-virus hoaxes, urban myths

#### 2004-08-23 Sweden king murder online hoax BBC Website impersonation spoof

NewsScan

KING CARL'S 'MURDER' AN ONLINE HOAX

Hoaxers have faked an announcement of the murder of the King of Sweden on a counterfeit BBC news website carrying a headline "Sweden's King Murdered" over a story saying that "Sweden's King Carl XVI Gustaf was shot in Athens this evening when he was on his way back to his hotel after

watching the Swedish table tennis star Jan-Ove Waldner beat Timo Boll, Germany, in the Olympic games." Swedish newspaper Expressen said the page had been sent by email to an unknown number of Hotmail e-mail addresses. "It's really very bad taste," the newspaper quoted a Royal Palace spokeswoman as saying: "It goes beyond the limit." Apart from the authentic-looking layout closely imitating the BBC, the news page also included genuine items such as the latest from Najaf in Iraq and the Olympics in order to enhance its appearance of credibility. (The Australian 23 Aug 2004) Rec'd fr J Lamp

# 1C1 Impersonation

Category1C1Impersonation2004-02-26e-mail spoofing stop solutions Microsoft Yahoo

NewsScan

PUTTING AN END TO SPOOFING

To stop Internet "spoofing"— the sending of mail from someone who pretends to be someone else — Microsoft and Yahoo are each developing systems aimed at authenticating senders of e-mail, as are companies such as America Online, Sendmail, Brightmail, and Amazon. Microsoft's proposal (Caller ID for E-mail) would require Internet service providers to submit lists of unique numeric addresses for their mail servers so that, on the message receiving end, software could check a database to verify that a message actually originated from one of its registered machines. Yahoo's proposal (DomainKeys) would use encryption to digitally sign messages, and if the sender or message content were altered the signature would get rejected. Experts predict that some combination of the techniques will be ready for use later this year. Margaret Olson of the Email Service Provider Coalition's technology committee says that once enough service and software providers adopt the technology, "getting unauthenticated mail delivered will be extremely difficult." (AP/USA Today 26 Feb 2004)

### Category 1C1 Impersonation

2004-03-01 electronic mail e-mail security privacy authentication identity spoofing

NIPC/DHS

February 26, Associated Press — Companies work on E- mail identity system.

With a simple adjustment in your e- mail software, you can pretend to be anyone. This is known as spoofing. To close that loophole, Microsoft and Yahoo! Inc. are each developing systems aimed at authenticating senders of E- mail. America Online is testing a third. "Having E- mail come in, and not really being able to identify where it comes from, this is a huge security hole," Bill Gates, of Microsoft, said this week in announcing specifications for his proposal. Microsoft's proposal, known as Caller ID for E- mail, calls for Internet service providers to submit lists of unique numeric addresses for their mail servers. On the receiving end, software would check a database to verify that a message said to come from an e- mail provider actually originated at one of its registered machines. In January, AOL began testing a similar system called Sender Policy Framework (SPF), which checks a different part of the message. Yahoo's proposed solution would use encryption to digitally sign messages. If the sender or message content is altered, the signature gets rejected. Issues to be worked out for all three systems include how to properly send E- mail from cybercafes, hotels, and public Wi- Fi hotspots and how to preserve privacy when using anonymous re- mailers, which are used by whistleblowers and others to intentionally mask the origin of messages.

#### Category 1C1 Impersonation

#### 2004-09-04 spoofing telephony caller-ID criminal hackers threats entrepreneur

NYT http://www.nytimes.com/2004/09/04/technology/04caller.html

Jason Jepson, an entrepreneur who tried to offer a commercial service that would have allowed callers such as debt collectors to fool callerID systems by feeding them incorrect identifying information -- spoofing the callerID system -- received a death threat along with harassing e-mail and phone calls and decided to abandon the idea only three days after his announcement. The company, Star38, would have charged a fee to trick call recipients into answering the phone and could have helped criminals trick victims into revealing confidential information under the mistaken belief that they were speaking to trustworthy callers based on the forged originating phone numbers.

# Category 1C1 Impersonation 2004-10-27 caller ID spoofing impersonation Website open security privacy implication White House call origination spoof

DHS IAIP Daily; http://www.securityfocus.com/news/9822

October 27, SecurityFocus — New Caller ID spoofing site opens.

A new Website offers subscribers a simple Web interface to a caller ID spoofing system that lets them appear to be calling from any number they choose. Called "Camophone," (www.camophone.com) the service functions much like the Star38.com (www.star38.com) site that struggled with an abortive launch last month: a user types in their phone number, the number they wish to call, and the number they'd like to wear as a disguise. The system instantly dials back and patches the call through with the properly- forged caller ID. The Star38.com site relaunched this week as a tool offered exclusively to law enforcement officials and "intelligence agencies." In contrast to Star38, Camophone is open to anyone with a PayPal account, at a rate of five cents per minute, pre- paid. The Camophone site performed as advertised in a test by SecurityFocus, in which a reporter made phone calls appear to originate from the White House switchboard.

## 1C2 Identity theft

Category 1C2 Identity theft

#### identity theft social security SSN video rental fraud Hollywood Video

NewsBits; http://www.usatoday.com/tech/news/2004-01-05-ssn-id-theft\_x.htm

Identity theft often begins with Social Security number

An article in USA Today for 15 January 2004 by William McCall of the Associated Press reviews excessive use of the Social Security Number. Despite increasing use of the identifier on commercial forms such as video-store rental applications, US residents have no legal obligation to reveal their SSN except for a few government, employment and fanking requirements. Retailers may refuse to grant services if a customer refuses to reveal the SSN, but the customer can take business elsewhere. Some untrained workers with access to SSN have been shown to reveal the information for unauthorized use; a reporter was able to acquire this information for two people with nothing more than providing his own street address.

2004-04-30	identity theft snail mail
Category 1C2	Identity theft

DHS IAIP Daily;

2004-01-05

http://www.stamfordadvocate.com/news/local/state/hc- 30081128.apds.m0926.bc - ct- brf- papr30,0,4492031.story?coll=hc- headlin es- local- wire

April 30, Associated Press - Postal clerk accused of identity theft.

A postal clerk in the Stamford, CT, police office has been charged with identity theft. Gail Worthington was arrested Wednesday, April 28, in a joint investigation by U.S. Postal Service inspectors and East Haven police. Worthington is accused of using information she obtained while at work to get credit cards in other people's names and use the cards to buy merchandise from high- end stores. The arrest was based on evidence found in a search of Worthington's East Haven apartment on March 10.

#### Category 1C2 Identity theft

#### 2004-05-01 identity theft phishing Internal Revenue Service IRS

DHS IAIP Daily;

http://edition.cnn.com/2004/TECH/internet/04/30/identity.the ft.ap/

May 01, Associated Press — IRS warns taxpayers about identity theft e- mails.

TheInternal Revenue Service (IRS) on Friday, April 30, warned consumers about an identity theft operation that tries to elicit personal information from taxpayers by sending e- mails alleging they're the subject of a tax investigation. Neither the Department of Treasury nor theInternal Revenue Service send e- mails to taxpayers about issues related to their accounts. The official- looking e- mail tells recipients they can dispute the tax fraud charge by logging onto a Website and providing detailed personal information like Social Security numbers, credit card numbers and driver's license numbers. Identity thieves use individuals' personal data to create false identification documents, to purchase goods and to apply for loans, credit cards or otherservices in the victim's name. The Internet service provider that hosted the fraudulent web siteshut it down at the request of the Treasury Department's inspector general for taxes. The IRS warns that new versions could surface.

Category 1C2 Identity theft

#### 2004-05-08 hacking identify theft university computer breach

DHS IAIP Daily;

http://www.fox23news.com/news/national/story.aspx?content\_id =5278A633- C320- 4F76- B1AB- AA431F5CAB16

May 08, Associated Press — Computer system at University of California, San Diego, hit by hackers.

Hackers broke into the computer system of the University of California, San Diego (UCSD), compromising confidential information on about 380,000 students, teachers, employees, alumni and applicants. Hackers infiltrated four computers that stored Social Security and driver's license numbers in the university's business and financial services department. Investigators are unaware of any illegal use of the data. University officials discovered the security breach April 16 after noticing a spike in traffic on the network. Last month, the San Diego Supercomputer Center, which is on the UCSD campus, was infiltrated by a hacker, although officials said no critical information was lost.

### Category1C2Identity theft2004-05-10identity theft social security numbers cards

DHS IAIP Daily;

http://www.suntimes.com/output/news/cst- nws- identity10.html

May 10, Chicago Sun- Times — State cracks down on identity theft.

In an effort to fight the growing problem of identity theft, the state of Illinois is cracking down on phony Social Security numbers on driver's licenses and ID cards. Secretary of State Jesse White said that Social Security numbers on four percent of Illinois driver's licenses and ID cards don't match records from the Social Security Administration. In many cases, there's no fraud involved. Examples of innocent mix- ups include motorists who use their middle names or change their names after getting married. However, from now on, motorists with suspect Social Security numbers will be required to prove their identity when they renew their licenses. The secretary of state is taking several other steps to combat identity fraud, in which someone steals the identity of someone else, often by assuming their name or other personal information. The office has stopped printing Social Security numbers on driver's licenses and is adopting more stringent document requirements. It also is using facial recognition programs that compare digital photos of motorists.

Category 1C2 Identity theft

#### 2004-05-11 identity theft paper trail victims

DHS IAIP Daily;

http://www1.redding.com/redd/nw\_local/article/0,2232,REDD\_17533\_2876398,00.html

May 11, Record Searchlight (CA) — Identity theft probe follows paper trail.

A former U.S. Bank employee arrested on suspicion of identity theft could be facing more charges in the near future. U.S. Bank's corporate security division is investigating Kenneth David Easley of Redding, CA, on suspicion of providing customer account information and counterfeit checks for others to cash, Redding police Sgt. Paul Grooms said Monday, May 10. "They're looking at victims throughout the West," he said. Easley was arrested April 8 following a month- long probe resulting in allegations that he gave account information and fake checks to three friends in Southern California. Grooms said Easley also is accused of creating counterfeit checks, although he would not say when, where or how he did it. Easley was a teller at the bank's main Redding branch. Approximately \$41,000 was stolen from two account holders at that branch and from another branch, Grooms said.

Category 1C2 Identity theft

2004-05-11 identity theft children fraud popularity increase

DHS IAIP Daily;

http://www.klas- tv.com/Global/story.asp?S=1859775&nav=168XN2 pW

May 11, KLAS- TV.com (NV) — Child identity theft gaining in popularity.

A new variation of identity theft is gaining in popularity, a variation law enforcement says is even tougher to crack. It's child identity theft - a crime that can go undetected for years. Identity theft expert Roy Michael says over the past five years, about 500,000 cases of child identity theft have been uncovered. However, half of those cases have come in the past two years. Children are targets because thieves can often get a 10 to 15 year head start on law enforcement. In fact, most children who've had their identity stolen don't know it until they someday go to apply for credit, a student loan, or buy a car. That's why identity theft experts say every parent should run a credit check on their child. A child's identity can sometimes get into the wrong hands through unsuspecting sources, for example, clubs or sports in which they participate, because they may require proof of age.

Category 1C2 Identity theft

#### 2004-05-13 identity theft victim assistance program Ohio

DHS IAIP Daily; http://www.nbc4columbus.com/money/3300186/detail.html

May 13, Nbc4columbus.com (OH) — Ohio gets grant to help identity theft victims.

The federal government gave the Ohio attorney general's office a \$250,000 grant to help implement a program aimed at assisting victims of identity theft, Attorney General Jim Petro announced Thursday, May 13. Petro said an Identity Theft Passport will be unveiled this summer that will allow victims to apply for a card when they file police reports with law enforcement agencies. The victims will be issued a card and certificate that can be shown to officers, creditors and others who question them. "The U.S. Department of Justice recognizes that our pilot program has the potential of being replicated nationwide," Petro said.

Category 1C2 Identity theft

2004-05-13 identity theft ring gang organized crime Colorado police

DHS IAIP Daily; http://www.koaa.com/news/view.asp?ID=2236

May 13, KOAA- TV (CO) — Identity theft ring closer to being solved.

Colorado Springs Police are closing in on the last of their organized crime suspects in the widespread identity theft case they've been working since last November. A 29- year- old man turned himself into Denver Police, after a warrant was issued last month for his arrest on Colorado organized crime charges. Three others have already been arrested. Investigators believe they ran a massive identity theft ring that included check forgery, credit card theft, car break- ins and burglaries, with hundreds of victims all across southern Colorado. Police say a number of the crimes are tied back to methanphetamine.

Category 1C2 Identity theft

#### 2004-05-17 identity theft banking scams phishing Australia bank Westpac

DHS IAIP Daily;

http://www.smh.com.au/articles/2004/05/17/1084646119834.html

May 17, Sydney Morning Herald (Australia) — Westpac targeted by more scams.

Australian bank Westpac is once again being targeted by e- mail scams which seek to extract usernames and passwords used for online banking. Two e- mails are doing the rounds, purportedly from Westpac Service Center or Westpac Support. Both attempt to lure unsuspecting souls to the same site: 207.150.192.12/temp/artsplos/secur.html. Only users of Internet Explorer are vulnerable to the scam. As soon as one inputs a username and password and clicks on the "sign- in" link, the genuine Westpac home page comes up.

Category 1C2 Identity theft

#### 2004-05-19 identity theft stolen social security numbers Utah

DHS IAIP Daily; http://www.4utah.com/local\_news/local\_headlines/story.aspx?c ontent\_id=6C104ABD- 79C2- 4BC4- 93FE- ED72A7D84923

May 19, ABC 4 (UT) — Scam using stolen social security numbers in Utah.

An ongoing investigation by federal and state agencies has found that 87 homes in Utah have been purchased using stolen Social Security numbers. So far, 21 individuals, all illegal immigrants, have been charged with felony crimes including identity theft, communications fraud, and forgery for their part in the scam. The scheme combines mortgage fraud with identity theft. Brokers target illegal immigrants in grocery store parking lots, and offer them the opportunity to buy a home despite their lack of credit or jobs. The undocumented workers then buy stolen Social Security numbers, which are used to find employment. The brokers, known as "flippers," then provide free down payments to the buyers, who use the Social Security numbers to qualify for mortgages. A lender then gives the buyer a loan based on an inflated appraisal of the home provided by an appraiser involved in the scheme. Eventually, the home buyer forecloses on the property and taxpayers are forced to cover the losses - all 87 homes purchased in Utah were federally insured through the U.S. Department of Housing and Urban Development.

Category 1C2 Identity theft

#### 2004-05-19 identity theft home security systems stealing customer data

http://www.reuters.com/newsArticle.jhtml?type=oddlyEnoughNew s&storyID=5193373

May 19, Reuters — Security provider jailed for identity theft.

A Connecticut man who installed home security systems has been sentenced to prison for using a client's personal information to finance a more than \$200,000 spending spree, federal prosecutors said. Kenneth Moore, who owned Security Plus Associates in North Haven, CT, was sentenced to 43 months in federal prison and three years probation on Monday, May 17. U.S. District Judge Stefan Underhill also ordered Moore to repay \$209,669.25. Moore used a client's name and social security number to secure financing for a \$41,420 fishing boat and a \$30,211 Mercedes Benz. He also opened credit card accounts with US Bank, First National Bank of Omaha, Shell Oil, Lowe's and Macy's. All of the cards were in the victim's name, but Moore provided his own address so the bills went to him, not the victim. Moore pleaded guilty to identity theft in February.

# Category 1C2 Identity theft 2004-07-15 identity theft legislation law George W. Bush President US prison criminals Internet cybercrime

NewsScan

BUSH SIGNS IDENTITY THEFT BILL

President Bush has signed into law an identity theft bill that will add two years to the prison sentences of criminals convicted of using stolen credit card numbers or other personal data to commit crimes. On top of that, the sentences of identity-theft violators who then commit acts of terrorism will be extended by an additional five years. The Federal Trade Commission estimates that 27.3 million Americans have been victims of identity theft in the last five years. (Washington Post 15 Jul 2004)

Category 1C2 Identity theft

#### 2004-07-16 personal private information theft device Australia ATM PIN

NewsScan

SMARTER SKIMMING DEVICE FOUND

A device designed to steal the personal details of ATM users was found in Sydney, Australia, by a customer who spotted the device and pulled it from the ATM. It had been in operation for three days, and may have recorded the confidential details of up to 1000 customers. The device, disguised to look like part of the ATM, uses a pin-hole camera to record the personal identification numbers of customers and a high-tech magnetic strip reader to steal the details on the card. Thieves can then use a decoder to burn the information onto any magnetic strip -- even a bus or train ticket -- and access users' bank balances. Police have found other machines used to rip off ATM users but the latest is by far the most hi-tech and devious. (The Australian, 16 Jul 2004) Rec'd from John Lamp

Category 1C2 Identity theft

#### 2004-08-26 identity theft I&A global crackdown US Department Justice John Ashcroft Federal Trade Commission FTC

NewsScan

GLOBAL CRACKDOWN ON IDENTITY THEFT

More than 100 people have been arrested and 53 convicted in a global ID theft crackdown dubbed "Operation Web Snare" coordinated by the U.S. Justice Department. The operation involved some 150,000 victims who lost more than \$215 million, according to Attorney General John Ashcroft -- a number he acknowledged represents only a small fraction of the crimes being committed on the Internet. Identity theft costs U.S. businesses more than \$50 billion a year. "The Internet is stimulating the development of innovative products and services that were barely imaginable only a few years ago," says Deborah Majoras, chairwoman of the FTC which also took

part in the operation. "There is a risk, however, that these benefits will not be fully realized if consumers associate the Internet with fraudulent operators." (Reuters/CNet 26 Aug 2004)

# Category 1C2 Identity theft 2004-10-27 ID identity theft Florida Chey Cobb Stephen Cobb public records Web disclosure access

NewsScan;

SAFE & SOUND IN THE CYBER AGE: FLORIDA'S ID THEFT KIT (by Chey Cobb & Stephen Cobb)

A few years ago, when the dot com bubble was still bubbling, legislators in the State of Florida got the 'technology bug' and mandated that all Florida counties put all public records on 'The Web.' We have no idea if the companies that make the hardware and software used to implement the mandate handed out campaign contributions to encourage this technology leap. But a lot of money has been spent on such technology in the years since, from dozens of high speed scanners to terabytes of storage and thousands of lines of Web code. The result? A large group of people, and even the country as a whole, is probably a lot less safe than it used to be. To understand why, take a look at a Web page we have put up to demonstrate: <http://www.privacyforbusiness.com/example1.htm> The link on the right shows you a prime example of what can happen when people don't fully grasp the relationship between privacy, technology, and human nature. Anyone on the planet with an Internet connection can now find intensely personal details about individuals who have lived in, or passed through, Florida. One such class of persons is elderly folk whose relatives have filed power of attorney (these records sometimes include banking data along with SSN and signature). Another worrying class of victims is U.S. military personnel. You can find out what their specialties are, their Social Security Numbers, addresses, relatives, signature, and so forth. The example we give is one of these, from Duval County, the most populous county in Florida. What you will see is the record as it appears on the Web, except that we added red ink to blot out key portions of the name of this particular person. If you go to the Duval County Web site, from any country in the world, you can find thousands of records just like this, with the name and SSN in place, NOT crossed out. Many of these people are not Florida residents, they just happen to have left the service while in Florida. The legislators who mandated this state of affairs were not alone in their failure to realize that "The Web" is the same "World Wide Web" you can access from anywhere, from Boca Raton to Bulgaria, Tampa Bay to Turkistan. A number of federal government agencies took the same leap off the cliff of commonsense in their eagerness to save money by automating public access to information. The basic mistake was to think of the Internet as the American public. Perhaps their Internet bubble was a Venn diagram in which the set of all U.S. citizens neatly coincided with the set of all Internet users. In the very early days of the Internet that might have been forgivable, but these days, when the evening news routinely pulls its footage from Islamic fundamentalist Web sites, you would think we'd all be a bit wiser. Apparently not. Consider how you get to these records, many of which are the perfect starting point for the crime of identity theft. You would think that you would need to know a specific person's name to find public records pertaining to them. But no, in Duval County you can simply ask to see all records of a particular type within a valid date range. In other counties you can't browse all records at once, but a very lame search mechanism lets you enter a single letter for a last name, like "A," and thus browse all persons whose name begins with "A," from Aarnem to Aziz. At some sites, including Duval, you don't even need a document viewer like Acrobat because the county provides one for you. Needless to say, we think this type of access to people's private information is wrong. Our government does not have the right to publish to the world our Social Security Numbers, signatures, and other personal details (and this doesn't even get into the whole issue of Florida juvenile records wrongly placed in the public domain). Things need to be changed. If anyone would like to contact us about efforts to effect changes we will try to do what we can to help. What sort of changes are needed? Well, expunging all Social Security Numbers would be a start, but even easier would be the requirement that you need to know the name of the person whose public records you are seeking. And personally, we see no reason for military discharge papers to be made available at the county level. Why not make that a responsibility of the branch of the armed services in which the person served? In the broader scheme of things Americans need to do some serious thinking about what 'public record' means. Stephen is sitting in a bar in Amsterdam right now, looking at military service records of people from Alabama to Wyoming. He's also viewing aerial photographs of properties in our Florida neighborhood, then pulling up the names and addresses of the owners, seeing what they paid for their homes and if their taxes are current. Does he have a right to do that? From there? And what about the fundamentalist who might be sitting next to him in that bar? [Chey Cobb, CISSP, the author of "Cryptography for Dummies" and "Network Security for Dummies," is a former senior technical security advisor to the NRO. Her email is chey at aug dot com. Stephen Cobb, CISSP, is the author of "Privacy for Business" and Chief Security Executive of STSN. His email is scobb at cobb dot com.]

# Category 1C2 Identity theft 2004-10-28 ID identity theft operation firewall international police Web identity forgery documents counterfeit data theft

NewsScan; http://www.washingtonpost.com/wp-dyn/articles/A7614-2004Oct28.html

IDENTITY THEFT SUSPECTS CAUGHT IN STING OPERATION

"Operation Firewall" -- an international law enforcement dragnet conducted by the U.S. Secret Service, the Justice and Homeland Security departments, the Royal Canadian Mounted Police, Europol and local police departments -- has led to the arrest of 28 individuals on suspicion of operating Web sites created to steal, sell and forge credit cards and ID documents. The sites operated under names such as Shadowcrew, Carderplanet and Darkprofits, and were hosted on multiple Internet servers outside the United States. The suspects are thought to have bought or sold about 1.7 million stolen information and counterfeit documents such as credit cards, driver's licenses, birth certificates and foreign and domestic passports. A MasterCard security executive familiar with the operations says, "We're talking about an international network that has new sites popping up all the time. These aren't high-tech individuals. All it takes is a computer, a little bit of knowledge, and these guys can do a lot of damage." (Washington Post 28 Oct 2004)

Category 1C2 Identity theft

#### 2004-11-22 ACLU passport ID identity theft microchips privacy

NewsScan; http://www.usatoday.com/tech/news/2004-11-22-hitech-

passport\_x.htm

ACLU ATTACKS MICROCHIP PASSPORT PLANS

The American Civil Liberties Union and some other privacy advocate groups are charging that international standards for "electronic" passports disregard a basic privacy approach protecting the security of the documents. New passports will have a chip containing the holders' name, birth date and issuing office, along with a "biometric" identifier that includes a photo of the holders' face. Barry Steinhardt of the ACLU says, "There's no security built into it. This will enable identity theft and put Americans at some risk when they travel internationally." A spokesman for the International Civil Aviation Organization and the State Department says those organizations are working on security concerns: "This is a process that is being implemented over the next few years, it is not something that happens overnight." The spokesman says that one way to fight identity theft is already in the standards, since the passports will have built-in encrypted authentication to let electronic readers know they are original documents and not forgeries. (AP/USA TODAY 22 Nov 2004)

# 1C3 Pseudonymity

Category 1C3 Pseudonymity

call blocking service privacy Star38 phone number masquerading spoofing caller ID

2004-09-02 NewsScan

SPY VERSUS SPY: UNBLOCK THAT CALL-BLOCK

A new computerized service from a company called Star38 will allow callers to create false outbound phone numbers and thereby fool call block software. Customers of the new service will be able to go to the company's Web site to enter the number they want to call and the number they want to appear on the caller ID screen of the recipient's phone. Some privacy-rights advocates are concerned that angry former spouses, stalkers or fraud artists could use the service for mischief, but Robert Atkinson of the Institute for Tele-Information at Columbia University, comments: "Some people see caller ID as an invasion of their privacy, while others see it as a protection of their privacy. It's spy versus spy." (New York Times 2 Sep 2004)

# 1C5 Phishing

Category 1C5Phishing2004-01-05phishing scam Bank of England e-mail fraud credit card moneyRISKS23

12

VISA CUSTOMERS HIT BY PHISHING EXPEDITION SEEMINGLY FROM BANK OF ENGLAND

RISKS 23.11 included a scrambled summary of a phishing scam; the correction in 23.12 from Simon Hogg included the following clarification:

As I'm sure many of the RISKs readers are aware, the Bank of England is a Central Bank and hence does not issue its own Visa (or any other credit cards) at least for consumers. Similarly, it doesn't operate consumer bank accounts. I suppose you could say that the Bank of England is equivalent to the Federal Reserve, \*not\* Bank of America. Therefore the BoE is unlikely to be a 'victim' in the ordinary sense of the word.

Therefore, I thought there was something a bit fishy with the PGN version saying that the "This was reportedly the first time BoE was victimized by a "phishing" expedition that apparently fooled about 5% of their Visa customers into divulging their card and PIN numbers."

Looking at the original news story the 'phishing' quote apparently relates to a different episode, "A campaign that targeted Visa credit card holders was said to have fooled one in 20 victims into divulging their personal details, including their card and pin numbers" \*i.e. not the BoE e-mail itself\*.

The point of the story is to say that lots of people were sent an e-mail with an executable attachment with the message "Please install our special software, that will remove all the keyloggers and backdoors from your computer." The implication (for the sender the hopeful implication) was that since the e-mail was apparently from the BoE, the software was in some way 'official'. Imagine the same e-mail in the US from someone@federal-reserve.gov.

I think the problem here is wider than a standard someone@aConsumerBank.com e-mail since it is apparently from a 'trusted' central bank (the one who controls the 'normal' banks) but it doesn't cause any direct 'damage' to the apparent sending agency.

So, three apparent risks;

1. Mis- / Dis-information (scaremongering?), accidental or otherwise, caused by incorrect summary of other news stories.

2. E-Mails apparently from a trusted source (common / usual RISKs here, but the 'trusted source' in this case is a 'super-trusted source').

3. For me the most worrying RISK is that the UK's "National High-Tech Crime Unit" came out with the very enlightening statement "We have opened the attachment, but we have so far not been able to find out what it does, if anything." How many programmers does it need to be able to analyse a piece of code to be able to work out what it does? Anti-virus labs are pretty good at this, so why not the Government-funded anti-crime 'specialists'? At least they are apparently being honest here(!).

Category 1C5 Phishing

2004-01-05 anti fraud phishing service UK Netcraft

NewsScan

A PROACTIVE APPROACH TO 'NO PHISHING'

Netcraft, based in the U.K., has launched an anti-fraud service aimed at preventing "phishing" — the practice of luring unsuspecting users to counterfeit banking sites where they're encouraged to divulge their credit card or other financial information. The company keeps a database of about 20 million home pages as well as a record of all registered Web site names. It then scours its copies of the Net's DNS records for suspicious entries related to or using its customers' name and alerts the legitimate name holder when it finds something. "It gives you the opportunity to try to pre-empt attacks," says Netcraft director Mike Prettejohn, rather than relying on customers to alert banks to online scams. (New Scientist 5 Jan 2004)

23

17

# Category1C5Phishing2004-01-28spam e-mail address hacking cracking images CAPTCHA pornography Website<br/>redirection phishing

RISKS

PORN VIEWERS WORK FOR HACKERS

Contributor Robin Burke summarizes an article about an online hack. Hackers are defeating the "CAPTCHAS" technique used to stop robots from registering for online services. Human beings can read what a CAPTCHA image asks for, and do its bidding, but robots can't because they're not intelligent enough. Now, hackers are "routing the CAPTCHA image to a page that advertises free porn." Viewers of these porn sites are given access to more free porn only after they decode a CAPTCHA image and complete a form to explain the image. Bots then use information from these porn-site forms to register for online services by seeming humanly intelligent.

Category 1C5	Phishing		
2004-02-04	phishing Internet Explorer fix patch URL		
RISKS		23	17
PHISHING AND A NEW IE SECURITY PATCH			

Contributor Sidney Markowitz notes that Microsoft has issued a security update to address an Internet Explorer phishing vulnerability. IE used to suppress portions of a URL after an '@', which was exploited by phishers to craft authentic-looking URLs. With this new patch, IE will suppress by default all URLs of the form "username:password@hostname". However, this can be changed in the Windows registry as needed.

Category 1C5 Phishing

2004-03-16 phishing scams corporate information risk steal business secrets

NewsScan

PHISHING SCAMS 'LIKELY TO TARGET CORPORATE INFO SOON'

Phishing scams will continue to flourish but their focus will change: they will increasingly target corporate information, the Asia-Pacific vice-president of one of the world's premier security company says. Richard Turner of RSA Security said the current rash of phishing scams was just the proverbial tip of the iceberg and those who were perpetrating them would turn to the more lucrative field of stealing business secrets. "Australian businesses are rapidly opening their networks to remote users, be they employees who want to work from home, customers or those from other companies who share information. As soon as you do this, you need to apply good policy to information systems and business systems," said Turner, who has been with RSA for the last eight years. "Once this stage is reached, the need to implement well-configured software becomes paramount, in order to provide protection against unauthorised connections." (The Age, 16 March 2004)

Category 1C5 Phishing

#### 2004-04-01 computer tools counter scams anti-phishing anti-fraud

DHS IAIP Daily;

http://story.news.yahoo.com/news?tmpl=story&cid=562&ncid=738 &e=2&u=/ap/20040401/ap\_on\_hi\_te/online\_scams

April 01, Associated Press — Companies sharpen tech tools to counter scams.

As Internet scams, also known as phishing, proliferate, companies are sharpening technological tools to counter them. Education alone, many agree, isn't enough. Anti- phishing software is apt to soon be added to the arsenal of digital shields forged to stop spam, viruses and hacking. Security companies are also building tools for banks and merchants to use behind the scenes. Phishing scams have been around for years but have in recent months become more numerous — and sophisticated. Scammers now copy and paste Web coding from real sites like Citibank's to give their fraudulent messages and the sites they lead to an aura of authenticity. They register Internet addresses that look real, subbing the letter "l" with the numeral "1," for instance. A few messages even carry ads for that aura of authenticity. The Anti- Phishing Working Group, formed in October by industry and law enforcement, identified 282 new phishing scams in February, up from 176 a month earlier. About 70 percent have been traced to eastern Europe or Asia, said David Jevans, the group's chairman.

### Category1C5Phishing2004-04-23fraud e-mail credit card banks FDIC personal information virus

NewsScan

BANKS WARNED ABOUT FRAUDULENT E-MAILS

The Federal Deposit Insurance Corp. (FDIC) is warning banks that consumers are receiving fraudulent e-mail messages claiming that the FDIC has collaborated with credit card providers to provide a new service and that by following a link in the message the recipient can get a free trial membership for discount coupons at various online retail outlets. The FDIC says: "The e-mail was not sent by the FDIC and may be a fraudulent attempt to obtain personal information from consumers or to implant a computer virus onto the recipient's computer. Financial institutions and consumers should not access the link or attached files provided in the body of the e-mail and should not, under any circumstances, provide any personal information to unknown sources." (AP/San Jose Mercury News 23 Apr 2004)

Category 1C5 Phishing

#### 2004-05-05 banking phishing fraud organized crime

DHS IAIP Daily; http://www.timesofmalta.com/core2/article.php?id=153129

May 05, Reuters — BIS warns of consumer banking scams using its name.

The Bank for International Settlements (BIS) on Tuesday, May 4, warned that its name and logo were being used in scams to defraud the public with offers of consumer banking services. The BIS is a central bank to the world's central banks. Its functions are purely official and it offers no services to private individuals or companies. "The BIS strongly cautions the public against sending money or disclosing bank or credit card details to any person who claims to represent the BIS or to have a banking relationship with the BIS," the bank said in a statement. The BIS named two "fraudulent websites" which are currently misusing its name, www.bfisonline.net and www.bisettlement.com. The BIS said fraud may be attempted via letter or e- mail as well.

Category 1C5 Phishing

#### 2004-05-05 banking phishing fraud organized crime

DHS IAIP Daily;

http://www.reuters.co.uk/newsArticle.jhtml?type=internetNews&storyID=504753 2&section=news

May 05, Reuters — Twelve held in phishing bank scam.

The National Hi- Tech Crime Unit of the United Kingdom (UK) Police have arrested a dozen Eastern European men and women on suspicion of defrauding UK online bank customers out of hundreds of thousands of pounds and diverting the money to a Russian crime gang. Some of the largest retail banks in the world, including Barclays, Lloyds TSB and NatWest in the UK, have been hit by the scam in which spoofed e- mails and Websites are used to trick online customers out of their bank and credit card details. Police say the group had money transferred from the defrauded accounts to bank accounts they had set up with false documents. They would then withdraw the money and ship it to Russia via wire transfers and money orders. Police described the suspects, whom they declined to name, as "mules" recruited by a single Russian organized crime gang to move the money out of a targeted country. Globally, the phishing crime wave has claimed victims in North America and Australia. The suspects are Estonian, Latvian, Russian and Ukrainian nationals. Also seized were computers and other electronic media, passports, check books and bank cards, money and crack cocaine.

Category1C5Phishing2004-05-05phishing credit card fraud internet café cyber café

DHS IAIP Daily; http://straitstimes.asia1.com.sg/asia/story/0,4386,249296,00

.html

May 05, The Straits Times (Singapore) — Online credit card fraud rocks Indonesia.

A briefing released by VeriSign, a U.S.- based company that monitors Internet activity, in January said that as more and more people around the globe go shopping online, the number of fraudulent transactions or transaction attempts has skyrocketed. An increasing number of fraud 4 attempts is being traced back to Indonesia. The VeriSign report also said that when researchers looked at the ratio of fraud attempts to total transactions from any single country, Indonesia topped the list. One reason why this type of crime is growing in Indonesia, experts said, is the proliferation in recent years of loosely regulated warnets, the local version of cybercafes. Most Indonesians cannot afford home computers and many who need to use the Web frequent the thousands of warnets in urban centers. Donny Budi Utoyo, of the Information Communication Technology Watch group, said, "the warnets do not keep a register of users and what they're doing while online. These kiosks present the perfect shields for offenders." The criminals' growing sophistication adds to the problem. Many criminals have formed syndicates with people living in other countries to better their chances of making money and avoid being traced.

Category 1C5 Phishing

#### 2004-05-05 phishing survey consumer confidence fraud

DHS IAIP Daily; http://www.theregister.co.uk/2004/05/05/phishing\_fears\_surve

y/

May 05, The Register (UK) — Fear of phishing hits e- commerce.

Concerns about falling victim to phishing scams are eroding U.S. consumer confidence in online banking and e- commerce. A survey out Tuesday, May 4, points to fears about online fraud based on widespread misconceptions about the minimal impact of phishing in overall fraud losses. Almost three in four online account holders responding to an online survey by software developer Cyota said they were less likely to shop online because of phishing. Cyota's poll revealing that 75 percent of account holders are less likely to respond to e- mail from their banks, and over 65 percent said they were less likely to sign up or continue to use their bank's online services as a result of fraud fears. Only 30 percent of the 650 respondents to the survey expressed a high level of confidence that they could distinguish between a real e- mail and a fraudulent one.

Category 1C5 Phishing

#### 2004-05-06 phishing banking scam theft

DHS IAIP Daily; http://www.reuters.com/newsArticle.jhtml?type=reutersEdge&st oryID=5062630

May 06, Reuters — Billions of phishing scam e- mails sent monthly.

Fraudulent e- mails designed to dupe Internet users out of their credit card details or bank information topped the three billion mark last month, according to one of the largest spam e- mail filtering companies. Over the past nine months, the monthly volume of phishing e- mails has risen nearly ten- fold to 3.1 billion worldwide in April, San Francisco, CA- based e- mail filtering firm Brightmail said. Brightmail said its spam filters sift through 96 billion e- mails each month. Police suspect organized crime gangs from Eastern Europe are the main culprits in the multi- billion dollar racket. The economic toll from phishing cost U.S. banks and credit card companies \$1.2 billion in 2003, Gartner Research said on Thursday, May 6. The Gartner study projected 1.78 million Americans reported giving personal information or financial details about themselves to the fraudsters. Police say the scam is concentrated on English- speaking countries such as the UK, U.S. and Australia, but is expected to target new territories as more people transact and bank online.

### Category1C5Phishing2004-05-14phishing banking identity theft trick

DHS IAIP Daily;

http://www.theage.com.au/articles/2004/05/14/1084289857949.h tml

May 14, The Age (Australia) — Phishers strike with a new trick.

Phishers in recent scam cases have created a fake address bar in the Web browser, making the e- mail look even more legitimate, according to a media release from the SurfControl Internet Research Center. The e- mail, targeting customers of US Bank, was issued on Wednesday, May 12. The Sydney- based research center says this new technique makes it even harder to identify if the e- mail is fake. In the latest scam, users who click the link in the spam e- mail are taken to a page that displays a fake address bar containing the real US Bank Website address. This address bar has been constructed to overlap the users existing address bar that normally identifies that the address was the scammer's server. Phishers use a Javascript code that calculates where the address bar is located on the user's Web browser, so it can be covered with the allegedly "legitimate" address details, the research center says.

Category 1C5 Phishing

#### 2004-05-18 phishing identity theft fraud email

DHS IAIP Daily; http://www.computerworld.com/securitytopics/security/cybercr ime/story/0,10801,93247,00.html

May 18, IDG News Service — Phishing scam reports skyrocket in April.

Reports of a type of online crime known as "phishing" surged last month, according to figures from a computer security industry group. The Anti- Phishing Working Group (APWG) received reports of more than 1,100 unique phishing campaigns in April, a 178% increase from the previous month, according to figures shared with the IDG News Service. The large increase comes on the heels of a 43% rise between February and March, and financial services and retail companies were hit particularly hard, said Dan Maier, director of product marketing at Louisville, KY- based Tumbleweed Inc. and an APWG spokesperson. Although each report recorded by the APWG corresponds to a unique phishing campaign, the type of attack that's used may not be new in every case, Maier said. In fact, the APWG has evidence that phishing Web pages are being traded online, in the same way that e- mail addresses are traded and sold by spammers. The growing problem also points to increasing interest in the scams by malicious hacking groups and organized crime, Maier said.

Category 1C5 Phishing

#### 2004-05-19 phishing identity theft fraud email

DHS IAIP Daily; http://www.kommersant.com/page.asp?id=475549

May 19, Kommerant (Russia) — Citibank Russia hit by phishing scam.

Citibank distributed a statement Tuesday, May 18, denying it was involved in a mass e- mailing of letters requesting more precise credit card information. A client who clicked on the link ended up on a phony Citibank Website where he was asked to enter his card number and PIN code. This type of fraud is known as "phishing," and was the first such case in Russia and a number of clients have already taken the bait. "These messages were actually sent to Citibank clients by frauds," the bank warns in its statement. Citibank's Russian branch was not only the first bank in Citigroup, but also in Russia to have these letters sent in its name. Citibank President Allan Hirst promised that, "in the event of receiving notification from clients of a loss of funds, Citibank is prepared to act in the interests of the client on an individual basis in evaluating each notification." However, the client's best chance of keeping his money in this case is to block the card on time.

Category 1C5 Phishing

### 2004-05-19 spammer caught texas man plead guilty luring people fake websites 46 months prison PayPal

NewsScan

SPAMMER GETS 46 MONTHS IN PRISON

A 20-year old Texas man who pleaded guilty of luring people to fake websites has been sentenced to 46 months in prison. The U.S. Justice Department said the sentence in Houston, Texas, for Zachary Keith Hill was linked to a phishing scam that used emails purported to come from AOL and the online payment service PayPal. The e-mail messages identified the sender as "billing center" or "account department" and the subject line carried warnings such as "AOL Billing Error Please Read Enclosed Email" or "Please Update Account Information Urgent!" (The Australian 19 May 2004) Rec'd from John Lamp, Deakin Univ.

#### Category 1C5 Phishing

#### 2004-05-21 phishing identity theft social engineering adjusting attacks

DHS IAIP Daily; http://www.finextra.com/fullstory.asp?id=11879

May 21, Finextra Research — Fake order confirmations provide new phishing twist.

UK security outfit SecureTest is warning of a new twist on the familiar phishing scam, in which fake e- mail order confirmations direct recipients to a Web server that writes a malicious file to the user's PC. The e- mail, a bogus order confirmation for an IBM Laptop PC, tells the recipient that their bank account has been debited for \$1969.03 and provides a link to check or cancel the order. Following the link leads to a Web server which exploits an unpatched weakness in Microsoft's Internet Explorer to write a potentially malicious file to the user's hard drive. Ken Munro, managing director at SecureTest, says the malicious code exploits a known threat which is listed by some of the major anti- virus vendors. "The danger here is in the new format for the scam, and the new form of social engineering," he says. "Many people, on receiving an e- mail saying their bank account has been debited for \$1969.03 will at least click on the link and take a further look."

#### Category 1C5 Phishing

#### identity theft credit offers snail mail financial services federal reserve

DHS IAIP Daily;

2004-05-26

http://www.yorkweekly.com/news/05262004/biz\_nati/18181.htm

May 26, Wall Street Journal — Federal Reserve scrutinizes credit offers.

With billions of credit solicitations mailed to consumers each year, the Federal Reserve is trying to figure out whether the offers for preapproved credit are fueling identity theft and encouraging consumers to take on excessive debt. While federal law lets lenders and insurance companies offer credit to consumers based on personal data from credit reports, the Federal Reserve is weighing whether the government needs to beef up a program that lets consumers block release of their credit reports. Evan Hendricks, editor of Privacy Times, a Washington- based newsletter, said it is easy for identity thieves to pick up preapproved solicitations by rifling through mailboxes. They can fill out the forms with a new address - - theirs - - and wait for the card to show up. While most credit companies won't send new cards to a new address, some credit unions and others do. Even if a thief can't obtain a credit card, the information in the solicitation itself is valuable, Hendricks said. An offer for a platinum card means a great credit rating, and a thief can sell that personal information to a "fence" who compiles the data and helps other identity thieves.

Category 1C5 Phishing

2004-05-26 phishing attack schemes alerts Department of Treasury

DHS IAIP Daily; http://gcn.com/vol1\_no1/daily- updates/26054- 1.html

May 26, Government Computer News — Treasury issues phishing schemes alert, advice.

The Department of Treasury on Wednesday, May 26, warned against schemes in which identity thieves spoof government agencies and financial firms to gain sensitive and financial information from unsuspecting consumers in a report that also offers some tips on how to prevent "phishing." Recent phishing e- mails have purportedly come from government agencies, legitimate financial- sector firms, Internet auction sites and electronic payment services. The government agencies include the Federal Deposit Insurance Corp., the Office of the Comptroller of the Currency, the Securities Investor Protection Corp. and others. A recent private- sector report found that 1,125 instances of phishing were reported in April, 180 percent more than in March. The report found that financial- services Websites are the most commonly spoofed. Treasury's report is on "Lessons Learned by Consumers, Financial Sector Firms, and Government Agencies during the Recent Rise of Phishing Attacks." "The report gives consumers even more information on how to detect, prevent and mitigate the effects of the identity theft scheme known as phishing, a crime that costs American consumers and businesses billions of dollars every year," said Assistant Secretary of Treasury Wayne Abernathy. Report: http://www.treas.gov/offices/domestic- financial- inst itution/cip/pdf/fbiic- fisscc- report- 2004.pdf.

### Category1C5Phishing2004-07-12pshishing cybercrime legislation US Senate jail fine scam fraud

NewsScan

THE PHIGHT AGAINST PHISHERS

The U.S. Senate is now considering legislation to fight "phishers" -- scam artists who use fake Web sites to dupe people into revealing their financial or other private information. The proposed law could cost phishers up to five years in jail and as much as \$250,000 in fines. Typically, a scammer who goes phishing will send a message doctored to look like an official notice from some respectable bank or online store, and will use the phony site to trick consumers into giving out their account information. Avivah Litan of Gartner Research warns: "The Internet's becoming a very dangerous place to conduct financial business unless you're willing to scrutinize your activities very closely." (Washington Post 12 Jul 2004)

#### Category 1C5 Phishing

#### 2004-12-09 phishing prediction confidentiality PhishNet defenses

NewsScan;

http://www.usatoday.com/tech/news/computersecurity/infotheft/2004-12-09-phish-starving\_x.htm

AN END TO PHISHING?

Former White House Web security chief Howard Schmidt, is predicting that "at this time next year" technology companies and law enforcement agencies will have forced an end to most kinds of Internet "phishing" scams that trick people into revealing their personal and financial information. Schmidt, who has worked with the group that created Digital PhishNet, promises that the major technology companies "are all working together to get the sites shut down as quickly as possible so they won't be around to collect your information." (Reuters/USA Today 9 Dec 2004)

### **Organizations, cooperation for law 1D1** enforcement

Category 1D1 Organizations, cooperation for law enforcement 2004-02-02

Internet fraud scam e-mail Nigerian 4-1-9 419 caught Netherlands

NewsScan

FINALLY! THE NIGERIAN E-MAIL SCAMMERS CAUGHT

Police in the Netherlands have arrested 52 people suspected of using the so-called "Nigerian e-mail scam" to defraud Internet users by sending them spam e-mails asking for their help in transferring a large sum of money out of Nigeria or some other troubled country in exchange for a generous percentage-fee. A task force of 80 officers raided 23 apartments, seizing computers, fake passports and 50,000 euros (\$62,000) in cash. Most of those arrested were believed to be Nigerian. (Wired 2 Feb 2004)

Category 1D1 Organizations, cooperation for law enforcement

#### 2004-05-17 Homeland Security DHS information sharing federal government

DHS IAIP Daily; http://www.govexec.com/dailyfed/0504/051404tdpm1.htm

May 17, National Journal's Technology Daily — Officials announce plan to share terrorism intelligence.

Attorney General John Ashcroft on Friday, May 14, unveiled an initiative to foster greater information sharing among federal, state and local law enforcement agencies. "No single government agency, or government, can win the war on terrorism," Ashcroft said. FBI Director Robert Mueller and Homeland Security Department Undersecretary Frank Libutti attended the announcement. Details of the National Criminal Intelligence Sharing Plan were developed at a 2002 law- enforcement summit convened by the International Association of Chiefs of Police to examine the requirements necessary for a national network that would gather, analyze and share information and intelligence on criminal and terrorist activities. On Friday, Ashcroft said the greatest structural failure in thwarting the September 11, 2001, terrorist attacks involved the "impediments to communication and information sharing among the men and women charged with keeping America safe.

Category 1D1	Organizations, cooperation for law enforcement
2004-06-22	Gypsy group lawsuit IBM Nazi Holocaust assistance compensation

NewsScan

GYPSY HOLOCAUST SURVIVORS SUING IBM IN SWISS COURT

Gypsies are suing IBM in Swiss court, alleging that IBM's expertise helped the Nazis commit mass murder more efficiently. A Gypsy group chose Geneva to file the lawsuit because IBM's wartime European headquarters were in that city. A Swiss appellate court has ruled: "IBM's complicity through material or intellectual assistance to the criminal acts of the Nazis during World War II via its Geneva office cannot be ruled out," and pointed to "a significant body of evidence indicating that the Geneva office could have been aware that it was assisting these acts." (AP/San Jose Mercury News 22 Jun 2004)

Category 1D1 Organizations, cooperation for law enforcement

2004-10-19 US Department of Justice DoJ hacking intellectual property rights target five units **CHIP** program

DHS IAIP Daily; http://sacramento.bizjournals.com/sacramento/stories/2004/10 /18/daily15.html

October 19, Sacramento Business Journal (CA) — Justice Department to target hacking, intellectual property theft with five new units.

The United States Attorney's office in five cities will be home to new Computer Hacking and Intellectual Property units, federal officials announced Tuesday, October 19. The new units, all in areas where intellectual property is a significant contributor to the economy, will be in Sacramento, CA; Washington, D.C.; Pittsburgh, PA; Nashville, TN; and Orlando, FL. The program, known as CHIP, will target copyright and trademark violations, theft of trade secrets, unauthorized access to computers, Internet fraud and theft of computers and other high- tech items. It will also train local law enforcement officers on tech issues. The new CHIP offices join 14 existing offices around the country.

2004-11-16	organized cybercrime Stephen Cobb Chey Cobb DHS federal
Category 1D1	Organizations, cooperation for law enforcement

NewsScan;

#### SAFE & SOUND IN THE CYBER AGE: FEDS TO THE RESCUE? By Stephen Cobb and Chey Cobb

Feds to the Rescue? Don't Hold Your Breath. First the bad news. If you were hoping that the threat of organized cybercrime would turn out to be something that we information security experts invented to drum up business, the time has come to stop hoping. International gangs of cyber-criminals do exist, as evidenced by the arrests announced recently by the U.S. Secret Service, which hauled in 28 people for alleged involvement in a global organized cybercrime ring (see NewsScan, 29 October 2004). According to the financial institutions victimized by this criminal enterprise, it netted more than \$4.3 million. The suspects, who come from six different countries in North America and Europe, are alleged to have trafficked "in at least 1.7 million stolen credit card numbers." According to Secret Service Director W. Ralph Basham, "These suspects targeted the personal and financial information of ordinary citizens, as well as the confidential and proprietary information of companies engaged in e-commerce." According to ComputerWorld, where Mr. Basham was quoted, the suspects operated Web sites that were used to buy and sell counterfeit credit cards and false identification documents, and also share information on how to commit fraud, trade in stolen information, and operate the tools needed to commit such crimes. We realize that the world today is full of big numbers, so if \$4.3 million doesn't strike you as a lot of money, bear in mind that this is just one bust of a few dozen felons. There are strong indications that hundreds, if not thousands, of criminals are getting in on the cybercrime wave. And there is little doubt that banks in the U.S. and Europe have lost several billions of dollars over the last twelve months to just one form of cybercrime: phishing (see Newsscan, 1 May 2003). A few months ago Gartner put the direct losses from phishing, that is, money fraudulently removed from people's account, at over \$2.4 billion, and sources in the UK cite losses of similar magnitude. So what's the good news? We don't think there is any, despite the admirable work of the Secret Service (assisted in this case by the U.K.'s National Hi-Tech Crimes Unit, the Vancouver Police Department's Financial Crimes Section, the Royal Canadian Mounted Police and Europol). Sadly, as hard as the fine officers of these agencies work, they are hardly making a dent in the problem (see the lead story in NewsScan Daily, 20 September 2004, for more on the scale of organized cybercrime). One reason for this lack of progress is undoubtedly the lack of government investment in basic cyber security research. Given the huge negative impact of cybercrimes on both U.S. citizens and U.S. financial institutions, you might expect the federal government to be pouring money into improving computer security. Sadly, according to experts in the field, the amount of federal funding for basic cyber security research is currently less than \$50 million a year (by comparison, the government recently contributed \$50 million to the building a rainforest in Iowa). Some say this disturbing situation was highlighted by the October resignation of Amit Yoran after just one year as director of the National Cyber Security Division of the Department of Homeland Security. This follows two previous high profile departures from the top cyber security post in less than two years (by Howard Schmidt and Richard Clarke respectively). Observers have cited a lack of funding as a major factor in all three resignations. One person who is very much in touch with this situation is Dr. Eugene Spafford, the executive director of the Center for Education and Research in Information Assurance and Security (CERIAS). Speaking at the Information Security Decisions conference in Chicago last month, Dr. Spafford surprised the audience of 500 information security practitioners with a multiple choice question: How much do you think the federal government is spending each year on basic computer security research? The responses, quickly tabulated by a very clever electronic audience feedback system, showed that most people assumed the government was spending a lot more than it really is. Always keen to give NewsScan readers the most accurate data, Stephen asked Dr. Spafford for clarification. After all, you might recall, as we did, the Cyber Security Research and Development Act of December, 2002, in which the President authorized up to \$903 million in cyber security research funds and fellowship opportunities at NSF and the National Institute of Standards and Technology (NIST), from 2003 through 2007. So how could spending be less than \$50 million per year? Sadly, replied Dr. Spafford, "Authorization is not appropriation... The authorization simply says that if the money is available to NSF, they can spend it. No additional money was actually appropriated." For readers interested in learning more, a report on cybersecurity research funding is due soon from PITAC, the President's Information Technology Advisory Committee,. It should show up here: http://www.itrd.gov/pitac/ index.html. If that report does not bear good news, you might want to contact your congresspersons, whomever they now may be. [Chey Cobb, CISSP, the author of "Network Security for Dummies," is a former senior technical security advisor to the NRO. Her email address is chev at soteira dot org. Stephen Cobb, CISSP, is the author of "Privacy for Business" and the Chief Security Executive at STSN. He can be reached as scobb at cobb dot com.]

Category 1D1 Organizations, cooperation for law enforcement

2004-11-17 Europe EU IT security cybercrime agency formed

DHS IAIP Daily; http://www.computerweekly.com/articles/article.asp?liArticle ID=135123&liArticleTypeID=1&liCategoryID=6&liChannelID=22&li FlavourID=1&sSearch=&nPage=1

November 17, ComputerWeekly — Europe's IT security agency set to fight cybercrime.

The European Union's international cybercrime squad is up and running, a year after it was given the go- ahead by the European Commission. The European Network and Information Security Agency (Enisa) has a five- year budget of \$44.5M and a mandate to get member states working together to combat security threats. It aims to become a pan- European "center of excellence" on security matters, collecting and analyzing data on security incidents, advising the commission and member states on security issues, standardizing security approaches and pushing for more co- operation between the private and public sectors.

## **1D2 Technology for law enforcement**

Category 1D2	Technology for law enforcement
2004-01-30	electronic cyber crime evidence destruction police business practice investigation United Kingdom UK

23

17

#### RISKS

UK: VITAL E-CRIME EVIDENCE OFTEN DESTROYED

Contributor Keith A. Rhodes presents an article from vnunet.com. The article states that some companies in the UK maybe destroying digital evidence on their systems while investigating cyber crimes before ringing for law enforcement help. The article reports that Len Hynds, the Detective Chief Superintendent of the National High Tech Crime Unit (NHTCU) said that there was a need to "...develop common standards in terms of dealing with high-tech crime between the private and public sectors." Michael Colao, a consultant, said: "What we see is well-meaning IT professionals going in and doing what you see on every bad crime film: they muddy the waters... You need a professional computer forensic team in there as soon as possible."

Category 1D2	Technology for law enforcement
2004-03-01	forensics police lab video separation manipulation

NewsScan

FORENSIC VIDEO

In Allegheny County, Pennsylvania, a police forensics lab is able to separate individual feeds from dozens of cameras that record on the same tape or disc and can stabilize images from shaky cameras and adjust the brightness and contrast. The techniques are similar to ones used by authorities in Florida to examine videotape from a car wash in Sarasota and help track down a man accused of abducting and killing an 11-year-old girl. But one of the officers in the Allegheny County lab cautions: "This is not a magic wand. There's a lot we can do with video and digital images, but there are still limitations." For example, although a surveillance camera outside a Pittsburgh job center captured the perpetration of a murder, police were unable to enhance the images enough to get a clear picture of the killer, causing one of the police offers to complain: "Frustrating isn't the word. You can see some facial features, his shoes, his distinct clothing, but it's just not enough." (AP/USA Today 1 Mar 2004)

Category 1D2 Technology for law enforcement

2004-04-01 Massachusetts open-standards open-source IT contract

DHS IAIP Daily; http://www.govtech.net/news/news.php?id=89839

April 01, Government Technology - Massachusetts awards first open- standards IT contract.

This week the state of Massachusetts acquired its first information technology (IT) services under its new open- standards policy. The Executive Department Legal Counsel's Virtual Law Office (VLO) will be developed using open- standards and open- source components. Similar to systems utilized by large private law firms, the VLO will deliver sophisticated content management, legal case management and new reporting tools. The contract award is expected to result in savings to the state both through more efficient management of legal services and outright ownership of the software code. Typically, state government would pay initial and ongoing licensing fees for new software. "The new open- standards policy is resulting in fair and open competition," said Administration and Finance Secretary Eric Kriss. "Out of the gate, this policy is having a positive impact on the state's bottom line."

Category 1D2 Technology for law enforcement

#### 2004-05-03 database law enforcement pharmaceutical FDA

DHS IAIP Daily; http://www.news- medical.net/view\_article.asp?id=1185

May 03, inpharma.com — Database to help identify counterfeit pharmaceuticals.

The Food and Drug Administration (FDA) is planning to create a database of the major pharmaceutical brands on the U.S. market, to make it easier to establish the authenticity of suspect products and identify counterfeit versions that enter the supply chain. The agency's Cincinnati- based Forensic Chemistry Centre (FCC) will establish a Counterfeit Analysis Work Group that will compile and maintain the database, which will contain frequently- updated information on both authentic brands and counterfeit versions of drugs. The group will put together a checklist that will be sent to all pharmaceutical companies selling products in the U.S., requiring them to provide the FCC with certain information about their brands to help ensure their authenticity. It will also create a database of authentic dosage forms for drugs. According to World Health Organization estimates, counterfeit medicines comprise six percent of the world market.

Category 1D2 Technology for law enforcement

#### 2004-05-24 wireless law enforcement automated dispatch

DHS IAIP Daily;

http://www.fcw.com/geb/articles/2004/0524/web- texwire- 05- 24- 04.asp

May 24, Federal Computer Week — Wireless to help Garland police.

The Garland, TX, police department will be the first local users of a new wireless network for first responders that is able to transmit voice and data at least 20 times faster than the city's old network. The deployment of the network will start with the city's 290 police officers, including the mobile data terminals in 80 squad cars. City officials are starting with data on the new network, using it as part of the Computer Automated Dispatch system to transmit 911 calls, alarms, report management, graphics and mug shots to the mobile units, said Darrell McClanahan, Garland's telecommunications manager. "This is an important milestone in fulfilling our city's communications vision for a fully converged high- speed data, voice and video network over which police, fire, emergency medical personnel and, eventually, all city employees will be interconnected in real time," McClanahan said.

Category 1D2 Technology for law enforcement

2004-06-23 law enforcement WiFi technology sting operations chat rooms pedophiles

NewsScan

MOBILE WIRELESS USED IN STING OPERATION

Law enforcement authorities in Texas have begun using a van equipped with high-speed wireless satellite devices to catch Internet surfers using chat rooms to set up illegal liaisons with underage girls. In the first sting operation in which the van has been used, seven men were apprehended

and charged with various felonious acts. A chief investigator in the Texas attorney general's office says, "In many of our rural areas, they lack the infrastructure we need to support this kind of investigation. So we now have the technology and ability to bring it with us. It's self-contained and

we're ready to go." (AP/USA Today 23 Jun 2004)

 Category
 1D2
 Technology for law enforcement

 2004-07-12
 Global Positioning System GPS Tennessee paroled offender tracking surveillance privacy freedom law enforcement technology

NewsScan

TENNESSEE GPS SYSTEM WILL TRACK PAROLED OFFENDERS

Tennessee has budgeted \$2.5 million for a pilot project that will test a global positioning system (GPS) for keeping track of paroled rapists. The system would let law enforcement build maps with "zones of exclusion" for the offenders (such as playgrounds, schools, day-care centers or the homes

of victims), and would allow probation officers to determine whether the felons they are supervising are going to work during the day, going home at night, and staying away from restricted areas. (The Tennessean 12 Jul 2004)

Category 1D2 Technology for law enforcement

#### 2004-10-18 privacy identification printers

NewsScan; http://news.bbc.co.uk/2/hi/technology/3753886.stm

EACH PRINTER CARRIES UNIQUE SIGNATURE

It turns out that every printer leaves a unique "intrinsic signature" on all the documents it produces, enabling law enforcement officials to track down printers used to make bogus bank notes, fake passports or other important documents. In a test, a research team from Purdue University was able to identify the correct printer more than 90% of the time. The signature derives from the way different printers lay down ink in distinct bands that can be spotted by image processing software. "We extract mathematical features, or measurements, from printed letters, then we use image analysis and pattern-recognition techniques to identify the printer," says Purdue professor Edward Delp. The research has been focused on identifying laserjet signatures, but the researchers are now turning their attention to inkjet printers as well.

2004-11-23	authentication artwork counterfeit law enforcement
Category 1D2	Technology for law enforcement

NewsScan;

http://www.cbc.ca/story/arts/national/2004/11/23/Arts/artcomputer041123.htm

l

COMPUTER AUTHENTICATION OF ARTWORKS

Computer scientists at Dartmouth College have developed a new mathematical process of authenticating art using highresolution digital photos and complex computer analyses to map out the idiosyncrasies of an artist's unique pen and brush stokes for comparison with other artworks. The process replicated the work of human authenticators when it was used to analyze works by artists Pieter Bruegel the Elder and Perugino. Dartmouth professor Hany Farid, co-director of the project, says: "What we've tried to do is capture certain mathematical properties of an artist in terms of their underlying style, properties almost certainly not visible to human eyes." But he emphasizes that the process is meant to be an additional tool, and not a replacement for the traditional means of authenticating artworks: "It's simply another tool that is contributing to the dialogue of art authenticating." (CBC News 23 Nov 2004)

Category 1D2 Technology for law enforcement

#### 2004-12-04 US intelligence search engine Convera homeland security data mining

NewsScan; http://www.washingtonpost.com/wp-dyn/articles/A30161-2004Dec2.html

THE SEARCH SOFTWARE USED BY THE IN-CROWD

Analysts working for U.S. intelligence and other federal agencies looking for documents and data stored on computers inside their own agencies they use software made by the Convera Corp. in Virginia, which offers specialized services and offer such features as the ability to automatically notify intelligence analysts when a new document matching a search query is added to the agency's database, and to search for patterns within data, identifying relationships buried in mountains of separate documents. Helen Mitchell, head of enterprise search for the FDA, says: "Before, people couldn't find everything if things were misfiled or they didn't have the time or resources. With the Convera software, and the technology for searching documents and patterns, they can find documents even with misspellings." Convera plans to make its Internet search engine available to regular computer users for free sometime next year. (Washington Post 4 Dec 2004)

Category 1D2 Technology for law enforcement

2004-12-05 cyber detectives DePaul University Chicago computer scientists pattern-recognition algorithm software crime detection neural network link CSSCP

DHS IAIP Daily; http://www.newscientist.com/news/news.jsp?id=ns99996734

December 05, New Scientist — Cyber detective links up crimes.

Computer scientists Tom Muscarello and Kamal Dahbur at DePaul University in Chicago have developed an artificial intelligence system that uses pattern- recognition software to link related crimes that may have taken place in widely separated areas whose police forces may rarely be in close contact. Called the Classification System for Serial Criminal Patterns (CSSCP), the system sifts through all the case records available to it, assigning numerical values to different aspects of each crime, such as the kind of offense, the perpetrator's sex, height and age, and the type of weapon or getaway vehicle used. From these figures it builds a crime description profile. A neural network program then uses this to seek out crimes with similar profiles. If it finds a possible link between two crimes, CSSCP compares when and where they took place to find out whether the same criminals would have had enough time to travel from one crime scene to the other. In the UK an online version of a manually searchable crime database called Crimelink was launched this week.

Category 1D2 Technology for law enforcement

### 2004-12-07 border checkpoints screening US photos scanning finger biometrics criminal databases

NewsScan; http://www.usatoday.com/tech/news/2004-12-07-border-printprogram\_x.htm ZIPPING THROUGH BORDER CHECKPOINTS

Foreigners entering the U.S. at some border crossings are now being processed by a new digital screening program that quickly scans photos of the traveler's face and index finger and matches them against federal agencies' criminal databases. Vistor Adolfo Moroyoqui Felix, traveling between Mexico and Phoenix, says: "It's much faster this way. They had to fill out paperwork before. It's more effective this way." Other travelers seem to agree. (AP/USA Today 7 Dec 2004)

Category 1D2 Technology for law enforcement

2004-12-12 data mining law enforcement research money laundering fraud financial crime

NYT http://www.nytimes.com/2004/12/12/politics/12finance.html

DHS ICE STUDIES DATA MINING TOOL

According to Eric Lichtblau, writing for the New York Times in December 2004, DHS (Department of Homeland Security) reported that the ICE (Immigration and Customs Enforcement) is studying a British database and program for data mining in financial transactions. The database from World-Check tracks a variety of financial crimes based on open-source information including 140,000 public sources; it already has information about roughly "250,000 people and firms with suspected ties to terrorist financing, drug trafficking, money laundering and other financial crimes."

Category 1D2 Technology for law enforcement

#### 2004-12-16 law enforcement Alabama tickets

NewsScan; http://apnews.excite.com/article/20041217/D8713ISO0.html

STATE TROOPERS ISSUING ELECTRONIC TICKETS

Well, it certainly cuts down on paperwork -- 50 Alabama state trooper vehicles are already equipped with laptops, scanners and printers that enable them to issue traffic tickets electronically and zap them directly to county courthouses rather than deliver them in person. Within two years, the state hopes to have the equipment in all 325 patrol cars, says state Public Safety Director Mike Coppage. Once e-citations are in use statewide, the next goal is to allow state troopers file accident investigation reports electronically and to enable them to access criminal records from their vehicles. (AP 16 Dec 2004)

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

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

2004-01-21 conviction underage sex solicitation email instant messaging monitoring

NewsBits; http://pennlive.com/newsflash/pa/index.ssf?/base/news-11/1074694141293801.xml

Court upholds conviction of man arrested because of e-mail

The Pennsylvania Supreme Court upheld the conviction of a man who says police should not have monitored his e-mail and instant messages without obtaining a court order. The case involved a former police officer, Robert Proetto, who was convicted of using the Internet to solicit sex from a 15-year-old girl. Proetto, a former officer with the Colonial Regional police in Northampton County, is appealing his conviction. The Supreme Court issued an order that merely affirmed a lower court's decision without comment.

EPIC ALERT 11.02:

## 1D4 Government funding for law enforcement

Category 1D4 Government funding for law enforcement

## 2004-01-16 Department Commerce IT security INFOSEC fund funding

NIPC/DHS;

http://www.fcw.com/fcw/articles/2004/0112/web- sade- 01- 14- 04. asp

January 14, Federal Computer Week — Commerce to fund IT security.

A senior Commerce Department official said funding will be poured into information technology security this year. Michael Sade, director for acquisition management and procurement executive, said the real impact of IT security isn't going to be on the technology side, but on the personnel side — such as ensuring vendors have security clearances. Sade generally spoke about how Commerce officials will better partner on projects with vendors and other government agencies through dialogue. Significant projects underway include modernization of the Patent and Trademark Office and National Weather Service. Commerce has begun making significant IT investment in preparation for the 2010 Census — possibly including the capability of doing surveys through the Web, Sade said. Another growing trend will entail better review of satellite programs in which the department funds projects that are overseen by other departments and agencies.

Category 1D4 Government funding for law enforcement

### 2004-02-26 security trade group cybersecurity advocacy Homeland Security Council

DHS IAIP Daily;

http://www.fcw.com/fcw/articles/2004/0223/web- security- 02- 26 - 04.asp

February 26, Federal Computer Week — Security trade group formed.

Eleven computer security companies announced the formation of an advocacy group, the Cyber Security Industry Alliance, to influence public policy and spending on cybersecurity. The members, which include well- known computer security firms, said they want to promote generally accepted information security principles, exchange cybersecurity threat information with government agencies, and eventually expand education and research to improve cybersecurity. Paul Kurtz was named executive director of the new organization. He is a former special assistant to the president and senior director of the Critical Infrastructure Protection Directorate under the White House's Homeland Security Council. Companies in the alliance are also interested in and supportive of the federal government's information technology product and systems certification program known as the National Information Assurance Partnership, said Ron Moritz, senior vice president and chief security strategist at Computer Associates International Inc.

Category 1D4 Government funding for law enforcement

### 2004-05-18 cybercrime law enforcement importance of skills

DHS IAIP Daily; http://news.zdnet.co.uk/internet/security/0,39020375,3915513 8,00.htm

May 18, ZDNet UK — Skills not money needed to fight cybercrime.

Law enforcement agencies require a bigger pool of skilled investigators and digital forensic experts, not more money or legislation, according to a study by The European Information Society Group (EURIM) that was presented at the House of Commons on Tuesday, May 18. According to the third phase of EURIM's e- crime study, around half the UK population and 10 percent of the world's population has access to the Internet. This means that a large number of criminals also connect to the Internet, which has led to the transfer of traditional crimes to the online world. The problem, said EURIM, is that although cybercrimes are becoming more common, members of the police force and specialist computer crime units lack many of the basic skills required to trace and analyze computer- based crimes. EURIM 's study makes a number of recommendations, one of which is to create specialist academic courses that focus on areas that are currently neglected by schools and colleges.

# Category 1D4 Government funding for law enforcement 2004-11-30 Federal Bureau Investigation FBI cybercrime security information technology student specialist recruitment challenge Internet Crime Complain Center I3C

DHS IAIP Daily;

http://www.eweek.com/article2/0,1759,1734035,00.asp?kc=ewnws120104dtx1k000 0599

November 30, eWeek — FBI's cyber- crime chief relates struggle for top talent.

The FBI's inability to recruit and keep the best available IT talent has proven to be one of the biggest challenges facing the government's Internet Crime Complaint Center (I3C), a senior official said Tuesday, November 30. Delivering the keynote address on the opening day of Ziff Davis Media's Security Virtual Tradeshow, I3C chief Daniel Larkin said the center's staffing problems underline the need for deeper cooperation between the FBI and the IT industry to win the battle against sophisticated cyber- criminals. "We can't recruit and keep the best available minds in the IT world. They come, stay a few years and move on because, ultimately, we can't pay what the industry pays for talent," Larkin said, adding that the bureau also has experienced difficulties with keeping pace with employees' training needs. Because of those shortcomings, Larkin said, the I3C spent the past four years forging partnerships with the biggest names in the tech industry to share expertise, coordinate on intelligence and develop best practices and protocols for fighting cyber- crime.

## 21.1 General QA failures

	-		
Category 21.1	General QA failures		
2004-01-05	QA quality assurance failure car registration computer alway	ys right	
RISKS		23	11
INPUT DATA ERROF	R ON TAG TRANSFER CAUSES DRIVER'S ARREST		
	n risks that a data entry error in processing a Maryland driver's car registrati deleted her records instead of transferring her registration to her new car.	on resulted in	n her arrest
Category 21.1	General QA failures		
2004-01-05	time_t 32-bit time software programs computers		
RISKS		23	12
HAPPY 2**30'TH BIR'	THDAY, TIME_T!		
32-bit counter counts se keeping time needed pat when time_t finally over order logic system, cause being discovered. In and	writes about the POSIX time counter time_t reaching half its positive rang conds elapsed since 1970. Some products by Parametric Technology Corp. ching because of the time_t half-time milestone. Eggert wonders how man flows in January 2038. Contributor Paul E. Black reports an overflow bug ed by time_t's birthday. The maintainers of Moscow ML issued patches wit ther follow-up article, Ed Ravin reports failure of the Heimdal implement in's company was able to work around this failure by upgrading to a newer	which were any applications in Moscow M thin a few day ation of Kert	using time_t for s will break IL, a higher /s of the bug peros because of
Category 21.1	General QA failures		
2004-01-14	Microsoft security bulletin patch flaw vulnerability fix buffer	overflow o	verrun
NIPC/DHS; http://www.microsof ulletin/MS04- 003.asj	t.com/technet/treeview/default.asp?url=/technet/security/b		
January 13, Microsoft — Execution (832483).	- Microsoft Security Bulletin MS04-003: Buffer Overrun in MDAC Function	on Could Alle	ow Code
number of database ope and that reside on the ne in a specific MDAC con buffer overflow. An att system as the program the SQL server that is on the vulnerable to an attack. enumerate computers the management tools instal	Components (MDAC) is a collection of components that provides the underations. When a client system on a network tries to see a list of computers stwork, it sends a broadcast request to all the devices that are on the netwo ponent, an attacker could respond to this request with a specially-crafted packer who successfully exploited this vulnerability could gain the same level hat initiated the broadcast request. For an attack to be successful an attack e same IP subnet as the target system. A target system must initiate such a An attacker would have no way of launching this first step but would have at are running SQL Server on the same subnet. Also, a system is not vulne led. Code executed on the client system would only run under the privileg nest. Microsoft has assigned a severity rating of "Important" to this issue.	that are runn rk. Because of backet that co l of privileges er would have broadcast ree to wait for a erable by havi	sover the e to simulate a quest to be nyone to ing these SQL
Category 21.1	General QA failures		
2004-02-08	design flaw data overrun field short digits quality assurance	failure QA	
RISKS; http://www.l	naaretzdaily.com/hasen/spages/392009.html	23	21
FIXED-LENGTH FIE	LDS STRIKE AGAIN		

Robert Israel reports on a design failure: >...the Israel Defense Forces will have to pay tens of millions of shekels to fix a twoyear-old automated system for calling up reservists: the system allocates 9 digits for a reservist's cell-phone number, but in a few months all Israeli cell phones will have 10 digits. According to the article, "The army will also look into expanding the fields for personal and other telephone numbers to prevent future problems."<

Category 21.1	General QA failures		
2004-02-11	power outage software flaw vulnerability General Electric GE management US blackout	software ene	ergy
RISKS		23	18
SOFTWARE BUG CO	NTRIBUTED TO BLACKOUT		
contributed to the Augu following the blackout. A "It [the software flaw] has the organization response	bulsen writes that a bug in General Electric (GE) energy management system st 14, 2003 northeastern US power blackout. The flaw was discovered from a A spokesman for Ohio-based FirstEnergy Corp., where the investigation into ad never evidenced itself until that day" The North American Electric Reli bible for preventing blackouts in the US and Canadaasked FirstEnergy to the C would start asking all electric companies in North America to patch their X	an in-depth sof the blackout b iability Council ioroughly patch	tware audit began, said: (NERC) 1 its XA/21
Category 21.1	General QA failures		
2004-02-25	quality assurance QA failure design problems toll system high	iway Germai	n autobahn
RISKS		23	21
TOLL COLLECT CONSORTIUM FAILS TO DELIVER			
Peter Ladkin provided a detailed report on the failure of a major industrial consortium to furnish the toll collection system for the German Autobahn network. Part of the problem may be traced to the unrealistic development schedule foisted on the winners of the Call for Proposals by government agencies. There were apparently also major design flaws such as inadequate interfacing with debit cards or the accounting systems used by major trucking firms. Losses are estimated in the billions of Euros.			
Category 21.1	General QA failures		
2004-02-27	heart monitor scanner physical reconfiguration design flaw		
RISKS		23	22
PACEMAKER REQUIRES OPERATION FOR RECONFIGURATION			

Nigel Metheringham noted in RISKS that a child was at risk of having an operation to replace a cardiac pacemaker so that a new monitor could be used after his original monitor was stolen. "The idea of an implantable medical device apparently requiring physical reconfiguration (at least) to talk to an external monitor implies a level of trust in the reliability of the external device which is seriously scary."

However, Dave Brunberg retorted in RISKS 23.24, "I think the RISKS of allowing unauthenticated remote reprogrammability of an implanted medical device may be just as scary. One way of reducing that RISK may be to have some sort of an "emergency broadcast" safe mode in which a new external monitor could identify itself to the implant and authorize through a highly secure key which would require knowledge of a passphrase to transmit. Of course, you'd really have to remember to change the default password...."

Category 21.1 General QA failures

### 2004-03-02 security vulnerability flaw hole patch fix WinZip MIME

DHS IAIP Daily; http://www.eweek.com/article2/0,4149,1540280,00.asp

February 27, eWEEK — Vulnerability in WinZip could compromise security.

Security analysts on Friday, February 27, reported that versions of the popular ZIP file management program WinZip have a serious security flaw. According to iDefense Inc., an error in the parameter parsing code in these versions "allows remote attackers to execute arbitrary code." The attacker would have to construct a specially designed MIME archive (with one of .mim, .uue, .uu, .b64, .bhx, .hqx and .xxe extensions) and distribute the file to users. Once opened, the attack would trick WinZip into executing code contained in the attacking file. iDefense said it had a functioning proof- of- concept attack demonstrating the problem. The malicious file could be distributed by e- mail, on a Web page, or through peer- to- peer networks. According to iDefense, versions 7 and 8, as well as the latest beta of WinZip 9 are vulnerable to this attack. However, the released Version 9 of WinZip is not vulnerable. In addition to upgrading, users can prevent an attack by turning off automatic handling of these file types by WinZip in Windows Explorer.

2004-03-31 new security vulnerability flaw hole buffer overflow exploit patch fix RealNetworks

DHS IAIP Daily; http://service.real.com/help/faq/security/security022604.html

March 26, eSecurity Planet — RealNetworks confirms buffer overflow problem.

Digital media delivery firm RealNetworks confirmed a buffer overflow vulnerability in its Helix Universal Server product, warning that a root exploit could give an attacker "inappropriate access" to compromised system. RealNetworks first warned of the flaw in January, describing it as a simple denial- of- service issue, but on Friday, March 26, the company released an updated advisory Friday to confirm the existence of a "potential root exploit." A root exploit could give an attacker complete control over a susceptible machine to execute malicious code. On Windows platforms where the Helix Server is run as an NT Service, the bug could allow arbitrary code execution under the context of the NT SYSTEM account. Vulnerable products includes Real's Helix Universal Mobile Server & Gateway 10, version 10.1.1.120 and prior and the Helix Universal Server and Gateway 9, version 9.0.2.881 and prior. RealNetworks has released an updated version of the Helix Universal Server or Gateway: http://service.real.com/help/faq/security/security022604.htm l

Category 21.1 General QA failures

## 2004-05-19 open source code repository flaw vulnerability

DHS IAIP Daily;

http://news.com.com/Flaws+found+in+manager+apps/2100- 1002\_3-5216353.html?tag=nefd.lede

May 19, CNET News.com — Flaws drill holes in open- source repository.

Flaws in two popular source code repository applications could allow attackers to access and corrupt open- source software projects, a security researcher said Wednesday, May 19. One vulnerability affects the Concurrent Versions System (CVS), an application used by many developers to store program code. The other flaw affects a system known as Subversion, said Stefan Esser, the researcher who discovered the security holes. The flaw in CVS, which is used more widely than Subversion, affects all versions of the software released before May 19, according to Esser. The vulnerability, technically known as a "heap overflow," occurs because data from the system's users is not vetted carefully enough. The CVS Project and major Linux and BSD distributions have posted advisories on the issue. The hole in Subversion is caused by an error in the way the code parses dates. It could be exploited to allow "remote code execution on Subversion servers and therefore could lead to a repository compromise," according to Esser's advisory.

Category 21.1 General QA failures

### 2004-05-26 vulnerability CVS buffer overflow concurrent version system

DHS IAIP Daily; http://www.us- cert.gov/cas/techalerts/TA04- 147A.html

May 26, US- CERT — Technical Cyber Security Alert TA04- 147A: CVS Heap Overflow Vulnerability.

There is a heap memory overflow vulnerability in the way CVS handles the insertion of modified and unchanged flags within entry lines. When processing an entry line, an additional byte of memory is allocated to flag the entry as modified or unchanged. There is a failure to check if a byte has been previously allocated for the flag, which creates an off- by- one buffer overflow. By calling a vulnerable function several times and inserting specific characters into the entry lines, a remote attacker could overwrite multiple blocks of memory. In some environments, the CVS server process is started by the Internet services daemon (inetd) and may run with root privileges. An authenticated client could exploit this vulnerability to execute arbitrary code, execute commands, modify sensitive information, or cause a denial of service. Note that if a CVS server is configured to permit anonymous read- only access, then this provides sufficient access to exploit a vulnerable server, as anonymous users are authenticated through the cvspserver process. Users should apply the appropriate patch or upgrade as specified by vendor. This issue has been resolved in Stable CVS Version 1.11.16 and CVS Feature Version 1.12.8.

## 2004-08-12 Adobe Acrobat Reader 5.0 UNIX Linux vulnerability command execution backtick character patch issued

DHS IAIP Daily;

http://www.idefense.com/application/poi/display?id=124&type=vulnerabilities&flashstatus=true

August 12, iDEFENSE — Adobe Acrobat Reader (Unix) shell metacharacter code execution vulnerability.

Remote exploitation of an input validation error in the uudecoding feature of Adobe Acrobat Reader (Unix) 5.0 allows an attacker to execute arbitrary code. The Unix and Linux versions of Adobe Acrobat Reader 5.0 automatically attempt to convert uuencoded documents back into their original format. The vulnerability specifically exists in the failure of Acrobat Reader to check for the backtick shell metacharacter in the filename before executing a command with a shell. Successful exploitation allows attackers to execute arbitrary code under the privileges of the user who opened the malicious document with a vulnerable version of Adobe Acrobat Reader. PDF documents are frequently exchanged via e- mail and in combination with a social engineering attack allows attackers to remotely exploit this vulnerability. Adobe Acrobat Reader (UNIX) 5.0.9 appears to be patched against this vulnerability.

# Category 21.1 General QA failures 2004-08-17 concurrent versioning system CVS history comand information disclosure vulnerability

DHS IAIP Daily; http://www.kb.cert.org/vuls/id/579225

August 17, US- CERT — Vulnerability Note VU#579225: CVS "history" command may disclose sensitive information.

Concurrent Versions System (CVS) is a source code maintenance system that is widely used by open- source software development projects. It provides a history command that displays reports on cvs commands that have been executed on files or directories in the source repository. When using the history command, it supports a - X command line switch, which is designed to allow a user to specify the name of the history file to be used. There is an information disclosure vulnerability in this command line switch. When specifying a directory or filename to the - X command line switch, the error message that is returned could allow an attacker to determine the existence and accessibility of arbitrary files or directories on an affected system. A remote, authenticated CVS user could determine if arbitrary files or directories exist on an affected system and whether the CVS daemon has 9 privileges to access them. This issue has been resolved in Stable CVS Version 1.11.17 and CVS Feature Version 1.12.9: https://www.cvshome.org/

Category 21.1 General QA failures

## Qt3 C++ programming library heap-based vulnerability

DHS IAIP Daily;

2004-08-18

http://www.mandrakesoft.com/security/advisories?name=MDKSA- 2 004:085

August 18, Mandrakesoft — Updated qt3 packages fix multiple vulnerabilities.

A heap- based overflow has been discovered in the QT library when handling 8- bit RLE encoded BMP files. This vulnerability could allow for the compromise of the account used to view or browse malicious BMP files. On subsequent investigation, it was also found that the handlers for XPM, GIF, and JPEG image types were also faulty. These problems affect all applications that use QT to handle image files, such as QT- based image viewers, the Konqueror web browser, and others. The updated packages have been patched to correct these problems.

Category 21.1 General QA failures

### 2004-08-21 **buffer heap overflow vulnerabilities XV file viewer**

DHS IAIP Daily; http://www.zone- h.org/advisories/read/id=5372

August 21, Zone- H.org — XV multiple buffer overflows.

XV contains at least five exploitable buffer and heap overflow vulnerabilities in the image handling code. This could allow an attacker to craft a malicious image, trick a user into viewing the file in xv, and upon viewing that image execute arbitrary code under privileges of the user viewing image. All versions may be affected. No workaround or solution is known at this time. Original Advisory: http://seclists.org/lists/bugtraq/2004/Aug/0275.html

## 2004-08-26 Winamp multimedia software skin file vulnerability code execution attack

DHS IAIP Daily; http://secunia.com/advisories/12381/

August 26, Secunia — Winamp skin file arbitrary code execution vulnerability.

A vulnerability exists in Winamp 5.04 which can be exploited by malicious people using a specially crafted Winamp skin to place and execute arbitrary programs. With Internet Explorer this can be done without user interaction. The problem is caused due to insufficient restrictions on Winamp skin zip files. The vulnerability has been confirmed on a fully patched system with Winamp 5.04 using Internet Explorer 6.0 on Microsoft Windows XP SP1. No solution is currently available.

Category 21.1 General QA failures

2004-08-26 Common Desktop Environment buffer overflow vulnerability information disclosure

DHS IAIP Daily;

http://www.idefense.com/application/poi/display?id=134&type=vulnerabilities&flashstatus=true

August 26, iDEFENSE — CDE libDtHelp LOGNAME buffer overflow vulnerability.

A buffer overflow vulnerability exists in the CDE libDtHelp LOGNAME variable that can allow local attackers to gain root privileges. CDE is a widely deployed default desktop environment for UNIX operating systems. Depending on the function of the machine, this vulnerability could lead to exposure of highly sensitive data. The vulnerability exists due to a lack of bounds checking on the LOGNAME environment variable. Patches addressing this issue are available from the various CDE vendors.

Category 21.1 General QA failures

### 2004-09-01 Oracle Database Application Server Enterprise Manager vulnerabilities

DHS IAIP Daily; http://www.uscert.gov/cas/techalerts/TA04- 245A.html

September 01, US- CERT — Technical Cyber Security Alert TA04- 245A: Multiple Vulnerabilities in Oracle Products.

Several vulnerabilities exist in the Oracle Database Server, Application Server, and Enterprise Manager software. The most serious vulnerabilities could allow a remote attacker to execute arbitrary code on an affected system. Oracle's Collaboration Suite and E- Business Suite 11i contain the vulnerable software and are affected as well. The impacts of these vulnerabilities range from the remote unauthenticated execution arbitrary code to data corruption or leakage. Vendor patches and updates are available: http://otn.oracle.com/deploy/security/pdf/2004alert68.pdf

Category 21.1 General QA failures

### 2004-09-02 Winzip ZIP file buffer overflow vulnerabilities exploit code execution attack

DHS IAIP Daily; http://secunia.com/advisories/12430/

September 02, Secunia — Winzip unspecified multiple buffer overflow vulnerabilities.

Multiple buffer overflow and input validation vulnerabilities exist in Winzip 9.0, which potentially can be exploited by a remote user to compromise a user's system. Successful exploitation can potentially lead to execution of arbitrary code. Update to 9.0 SR- 1: http://www.winzip.com/upgrade.htm

# Category 21.1 General QA failures 2004-09-02 DB2 Universal Database software buffer overflow vulnerabilities fixpacs updates issued

DHS IAIP Daily; http://www.securitytracker.com/alerts/2004/Sep/1011140.html

September 02, SecurityTracker — DB2 multiple unspecified vulnerabilities.

Multiple unspecified vulnerabilities exist in DB2 Universal Database, allowing malicious people to compromise a vulnerable system. Two of the vulnerabilities are caused due to boundary errors, which can be exploited by a remote user to execute arbitrary code. There are also some other unspecified errors with an unknown impact. The vendor has issued fixpaks, which address the two buffer overflow vulnerabilities: DB2 8.1:

http://www- 306.ibm.com/software/data/db2/udb/support/downloa dv8.html and DB2 7.x:

http://www- 306.ibm.com/software/data/db2/udb/support/downloa dv7.html

2004-09-08 mpg123 MPEG layer-2 audio decoder buffer overflow vulnerability no update issued

DHS IAIP Daily; http://secunia.com/advisories/12478/

September 08, Secunia — mpg123 Mpeg Layer- 2 audio decoder buffer overflow vulnerability.

A buffer overflow vulnerability exists in mpg123 version 0.59r. Successful exploitation may allow execution of arbitrary code with the privileges of the user executing mpg123. No vendor solution is currently available.

	Category	21.1	General QA failures
--	----------	------	---------------------

### 2004-09-08 Usermin vulnerabilities open source command execution

DHS IAIP Daily; http://secunia.com/advisories/12488/

September 08, Secunia — Usermin shell command injection and insecure installation vulnerabilities.

Two vulnerabilities have been reported in Usermin, where the most critical can be exploited to permit malicious people to execute arbitrary commands with the privileges of the Usermin user. Update to version 1.090: http://www.webmin.com/index6.html

Category 21.1 General QA failures

### 2004-09-30 Samba input validation vulnerability file access attack

DHS IAIP Daily;

http://www.idefense.com/application/poi/display?id=146&type=vulnerabilities&flashstatus=true

September 30, iDEFENSE — Samba arbitrary file access vulnerability.

An input validation vulnerability has been reported in Samba 3.0.2 and 2.2.9 which allows attackers to remotely access files and directories outside of the specified share path. An attacker does not need exploit code to exploit this vulnerability. Vendor upgrades available at: http://us4.samba.org/samba

## Category 21.1 General QA failures

### 2004-10-06 DB2 database vulnerabilities denial of service DoS

DHS IAIP Daily; http://secunia.com/advisories/12733/

October 06, Secunia — DB2 Universal Database multiple vulnerabilities.

Multiple vulnerabilities have been reported in DB2 Universal Database, where some of the vulnerabilities can be exploited to cause a Denial of Service, system access, or execution of arbitrary code. Apply DB2 FixPak 6a or 7a: http://www- 306.ibm.com/software/data/db2/udb/support/downloa dv8.html. Fixes for DB2 7.2 will be included in FixPak 13.

Category 21.1 General QA failures

## 2004-10-08 SANS top 20 Internet security vulnerabilities list

DHS IAIP Daily; http://security.itworld.com/4341/041008sanstop20/page\_1.html

October 08, IDG News Service — SANS unveils top 20 security vulnerabilities.

IT security and research organization The SANS Institute released its annual Top 20 list of Internet security vulnerabilities on Friday, October 8, with the intention of offering organizations at least a starting point for addressing critical issues. The SANS list is compiled from recommendations by leading security researchers, companies, and government organizations around the world. The list is divided into the top 10 Windows and top 10 Unix vulnerabilities. Topping the Windows list is Web servers and services, while the Unix list leads with BIND domain name systems. Vulnerabilities in file sharing applications and instant messaging (IM), which ranked seven and 10 on the Windows list, respectively, represent fairly new categories of risk, said Ross Patel, director of the Top 20 list. Report: http://www.sans.org/top20/

2004-10-13 Adobe Acrobat Reader information disclosure vulnerability no update issued

DHS IAIP Daily; http://secunia.com/advisories/12809/

October 13, Secunia — Adobe Acrobat / Adobe Reader disclosure of sensitive information.

A vulnerability has been discovered in Adobe Acrobat and Adobe Reader, which can be exploited by malicious people to disclose sensitive information. The problem is that embedded Macromedia flash files can be executed in a local context. There is no vendor solution at this time.

Category 21.1 General QA failures

## 2004-10-15 **Oracle database vulnerability exploits software patches available**

DHS IAIP Daily; http://www.nwfusion.com/news/2004/1015oraclwarns.html

October 15, IDG News Service — Oracle warns of exploits for latest database flaws.

Oracle is warning customers to apply software patches it released in August 2004, citing the availability of malicious code that can exploit unpatched vulnerabilities in its software. The security holes affect a number of Oracle products, including Versions of its 8i, 9i and 10g Database, Application Server and Enterprise Manager software. Oracle strongly recommends affected customers apply the software patches "without delay."

Category 21.1 General QA failures

## 2004-10-19 Lotus Notes Domino cross site scripting attack vulnerability no update issued

DHS IAIP Daily; http://securitytracker.com/alerts/2004/Oct/1011779.html

October 19, SecurityTracker — Lotus Notes/Domino square bracket encoding failure lets remote users conduct cross- site scripting attacks.

A remote user can access the target user's cookies (including authentication cookies), if any, associated with the site running the Notes/Domino software, access data recently submitted by the target user via web form to the site, or take actions on the site acting as the target user. It is reported that the Lotus Notes HTML encoding function fails to encode square brackets ('[' and ']'). No solution is currently available.

Category 21.1 General QA failures

### 2004-10-26 Novell ZENworks privilege escalation vulnerability Remote Management Agent

DHS IAIP Daily; http://secunia.com/advisories/12969/

October 26, Secunia — Novell ZENworks for Desktops privilege escalation vulnerability.

A vulnerability exists in Novell ZENworks for Desktops, which can be exploited by malicious, local users to gain escalated privileges. The vulnerability is caused due to the Remote Management Agent invoking the ZENworks Remote Control Help functionality with SYSTEM privileges. This can be exploited to execute arbitrary programs with escalated privileges. The vulnerability has been fixed in version 4 SP1b/4.0.1 Interim Release 5: http://support.novell.com/servlet/filedownload/sec/pub/zfd40 1\_ir5.exe

Category 21.1 General QA failures

## 2004-10-27 **RealPlayer skin buffer overflow vulnerability code execution attack**

DHS IAIP Daily; http://www.securitytracker.com/alerts/2004/Oct/1011944.html

October 27, SecurityTracker — RealPlayer skin file buffer overflow may let remote users run arbitrary code.

RealNetworks reported that a remote user can create a malicious skin file that, when loaded by the target user, will trigger a buffer overflow in DUNZIP32.DLL and potentially execute arbitrary code. A fixed version (10.5 (6.0.12.1056)) is available: www.service.real.com/help/faq/security/041026\_player/

## 2004-10-28 QuickTime software heap based buffer overflow vulnerabilities HTML BMP

DHS IAIP Daily; http://secunia.com/advisories/13005/l

October 28, Secunia — Two Quicktime vulnerabilities.

An unspecified integer overflow can be exploited in Quicktime to cause a buffer overflow and execute arbitrary code on a user's system via a specially crafted HTML document. Also, a boundary error within the decoding of BMP images can be exploited to cause a heap- based buffer overflow and execute arbitrary code on a user's system. The integer overflow only effects Windows systems. Update to version 6.5.2: http://www.apple.com/support/downloads/quicktime.html

## Category 21.1 General QA failures

## 2004-11-04 Google local service cross site scripting vulnerability no update issued

DHS IAIP Daily; http://www.zone- h.org/advisories/read/id=6180

November 04, Zone- H.org — Cross Site Scripting vulnerability in Google Local service.

An input validation vulnerability has been reported in Google Local service. A remote user can access the target user's cookies (including authentication cookies), if any, associated with the Google Local site, access data recently submitted by the target user via Web form to the site, or take actions on the site acting as the target user. There is no solution at this time.

Category	21.1	General QA failures
----------	------	---------------------

## 2004-11-23 Winamp stack based buffer overflow vulnerability code execution

DHS IAIP Daily; http://secunia.com/advisories/13269/

November 23, Secunia — Winamp "IN\_CDDA.dll" buffer overflow vulnerability.

A vulnerability in Winamp 5.05 has been reported which can be exploited by malicious people to compromise a user's system. The vulnerability is caused due to a boundary error in the "IN\_CDDA.dll" file. This can be exploited in various ways to cause a stack- based buffer overflow, e.g., by tricking a user into visiting a malicious web site containing a specially crafted ".m3u" playlist. Successful exploitation allows execution of arbitrary code. Update to version 5.0.6: http://www.winamp.com/player/

Category 21.1 General QA failures

## 2004-12-16 Veritas backup software registration stack based buffer overflow vulnerability code execution attack update issued

DHS IAIP Daily; http://secunia.com/advisories/13495/

December 16, Secunia — Veritas Backup Exec registration request buffer overflow.

A vulnerability has been reported in VERITAS Backup Exec, which can be exploited by malicious people to compromise a vulnerable system. The vulnerability is caused due to a boundary error in the Agent Browser service when processing received registration requests and can be exploited to cause a stack- based buffer overflow. Successful exploitation allows execution of arbitrary code. Original advisory and hotfixes available at: http://seer.support.veritas.com/docs/273419.htm

Category 21.1 General QA failures

## 2004-12-21 libtiff TIFF integer overflow vulnerability code execution attack update issued

DHS IAIP Daily;

http://www.idefense.com/application/poi/display?id=174&type= vulnerabilities

December 21, iDEFENSE — Libtiff directory entry count integer overflow vulnerability.

Remote attackers may be able to execute arbitrary code with permissions of the user opening the malformed TIFF file. The exposure to this vulnerability is mitigated by the fact that user interaction is required and that the user must view the malicious TIFF file in an application that is linked to a vulnerable version of libtiff. Update to version 3.7.1. ftp://ftp.remotesensing.org/pub/libtiff/

## 2004-12-22 Xpdf buffer overflow vulnerability code execution attack update issued

DHS IAIP Daily; http://secunia.com/advisories/13602/

December 22, Secunia — Xpdf "doImage()" Buffer Overflow Vulnerability.

A vulnerability has been reported in xpdf, which can be exploited by malicious people to compromise a user's system. The vulnerability is caused due to a boundary error in the "doImage()" function in "Gfx.cc". This can be exploited to cause a buffer overflow by tricking a user into opening a malicious PDF file.Successful exploitation may allow execution of arbitrary code. Apply patch for version 3.00: ftp://ftp.foolabs.com/pub/xpdf/xpdf- 3.00pl2.patch Update to version 3.00pl2. http://www.foolabs.com/xpdf/download.html

Category 21.1 General QA failures

## 2004-12-30 WHM application software AutoPilot multiple vulnerabilities cross site scripting attack update issued

DHS IAIP Daily; http://secunia.com/advisories/13673/

December 30, Secunia — WHM AutoPilot multiple vulnerabilities.

WHM AutoPilot has some vulnerabilities that can be exploited by malicious people to conduct cross- site scripting, this allows hackers to compromise a vulnerable system and disclose system information. Input passed to the "site\_title" and "http\_images" parameter in "header.php" isn't properly sanitized before being returned to the user. This can be exploited to execute arbitrary HTML and script code in a user's browser session in context of a vulnerable site. Update to version 2.5.0: http://www.whmautopilot.com/

## **Security product QA failures** 21.2

Category 21.2 Security product QA failures

2004-01-09 password protection MS Word document bug failure weakness flaw

## RISKS:

http://news.zdnet.co.uk/software/windows/0,39020396,39118935,00.htm=20

12

23

'UNFIXABLE' WORD PASSWORD HOLE EXPOSED

Brett McCarron reports as follows:

The password used to "protect" a Microsoft Word form can be revealed with a simple text editor, according to a recent BugTraq article. The RISK in this case goes beyond the ability to edit a protected document (you can bypass this anyway with Edit > Select All > Copy, open a new document and Paste). The real RISK is that the user's password is so easy to discover. Ideally, users would protect a form with a password that is different from their network authentication password(s). But in the real word ...

News Story

http://news.zdnet.co.uk/software/windows/0,39020396,39118935,00.htm=20

**BugTraq** Article

http://www.securityfocus.com/archive/1/348692/2004-01-02/2004-01-08/0

Category 21.2 Security product QA failures

2004-01-14 Microsoft security bulletin patch flaw vulnerability fix

NIPC/DHS:

http://www.microsoft.com/technet/treeview/default.asp?url=/technet/security/b ulletin/MS04-001.asp

January 13, Microsoft — Microsoft Security Bulletin MS04-001: Vulnerability in Microsoft Internet Security and Acceleration Server 2000 H.323 Filter Can Allow Remote Code Execution.

A security vulnerability exists in the H.323 filter for Microsoft Internet Security and Acceleration Server 2000 that could allow an attacker to overflow a buffer in the Microsoft Firewall Service in Microsoft Internet Security and Acceleration Server 2000. An attacker who successfully exploited this vulnerability could try to run code of their choice in the security context of the Microsoft Firewall Service. This would give the attacker complete control over the system. The H.323 filter is enabled by default on servers running ISA Server 2000 computers that are installed in integrated or firewall mode. ISA Servers running in cache mode are not vulnerable because the Microsoft Firewall Service is disabled by default. Users can prevent the risk of attack by disabling the H.323 filter. Microsoft has assigned a severity rating of "Critical" to this issue.

Category 21.2 Security product QA failures

2004-01-28 US-CERT CERT warning forget operating system OS worm vulnerability RISKS 23 15 US-CERT WARNS OF WORM, FORGETS TO MENTION OPERATING SYSTEM

Contributor Kevin Dalley reports that US-CERT published a warning about the MyDoom.B worm but forgot to mention explicitly what the susceptible operating system was: http://www.us-cert.gov/cas/techalerts/TA04-028A.html CERT issued a warning for the Novarg A worm, titled "Steps for Recovering from a UNIX or NT System Compromise." With warning, says Dalley, at least "one could assume that UNIX is at risk." Dalley finishes: "Chew on these CERTs and you will be lucky to see a spark of light."

# Category 21.2 Security product QA failures 2004-02-05 VPN ISS firewalls proxy HTTP request check point Application Intelligence AI update issued

DHS IAIP Daily;

http://www.crn.com/sections/BreakingNews/dailyarchives.asp?A rticleID=47735

February 05, TechWeb — Security flaws found in popular firewall software.

Flaws found late Wednesday in Check Point Software's popular firewall and VPN software could allow an attacker to gain entrance to enterprise networks, Internet Security Systems (ISS) said in a critical alert. The disclosure of the vulnerabilities is yet another sign of a move by hackers to hammer at security software, firewalls, and intrusion detection systems, the very devices and applications enterprises rely on to defend themselves against intruders, said Dan Ingevaldson, the director of ISS's X- Force research team. The first vulnerability is within Check Point Firewall- 1, and stems from the HTTP Application Intelligence that's designed to prevent potential attacks or detect protocol anomalies aimed at servers behind the firewall. The flaw also exists in the HTTP Security Server applications proxy that ships with all versions of Firewall- 1, including the most recent. On Wednesday, Check Point posted a patch for this vulnerability that it recommended be installed immediately. The second vulnerability lies within Check Point VPN- 1 Server and its virtual private networking (VPN) clients, Securemote and SecureClient. The vulnerability exists in the ISAKMP processing in both the server and clients, and if exploited, could result in an attacker gaining access to any client- enabled remote computer, including those in employees' homes.

Category 21.2 Security product QA failures

2004-02-05 firewalls proxy HTTP request check point Application Intelligence AI update issued

DHS IAIP Daily; http://www.us- cert.gov/cas/techalerts/TA04- 036A.html

February 05, US- CERT — Technical Cyber Security Alert TA04- 036A: HTTP Parsing Vulnerabilities in Check Point Firewall- 1.

The Application Intelligence (AI) component of Check Point Firewall- 1 is an application proxy that scans traffic for application layer attacks once it has passed through the firewall at the network level. Both the AI and HTTP Security Server features contain an HTTP parsing vulnerability that is triggered by sending an invalid HTTP request through the firewall. When Firewall- 1 generates an error message in response to the invalid request, a portion of the input supplied by the attacker is included in the format string for a call to sprintf(). It is possible to exploit this format string vulnerability to execute commands on the firewall. This vulnerability can be exploited as a heap overflow, which would allow an attacker to execute arbitrary code. In either case, the commands or code executed by the attacker would run with administrative privileges, typically "SYSTEM" or "root". Additional information and a patch are available on the Check Point Website: http://www.checkpoint.com/techsupport/alerts/security\_server.html

Category 21.2 Security product QA failures

## 2004-03-02 security vulnerability flaw hole fix patch Dell OpenManage server HTTP POST

DHS IAIP Daily;

http://www.techworld.com/news/index.cfm?fuseaction=displaynews&NewsID=11 15

February 27, Techworld — Critical security hole in Dell OpenManage.

A security hole in Dell OpenManage server could leave the product open to attack by an unauthorized user. The problem has been identified as high risk by security consultancy Secunia. The vulnerability is caused due to a boundary error in the Web server when handling certain HTTP POST requests. POST is an extremely common HTML method of processing forms but can be exploited by sending a message with a hidden but extremely long variable to cause a heap overflow. The vulnerability can be side- stepped by restricting access to Port 1311/TCP and only allowing trusted IP addresses to connect. However, without that in place, a denial of service or system access are readily achievable. Additional information is available on the Secunia Website: http://secunia.com/advisories/10994/

## Category21.2Security product QA failures2004-03-22security vulnerability flaw hole patch fix Norton Internet software

## DHS IAIP Daily;

March 19, CNET News.com — Flaw stymies Norton Internet Security.

A software component of Norton Internet Security could allow hackers to use the application as a backdoor into a person's computer system, security researchers warned Friday, March 19. The flaw occurs in an ActiveX component used by security firm Symantec's desktop security program, Norton Internet Security, according to research firm NGSSoftware. The security hole could be used to run an attack program that would then take control of the computer that the software was trying to protect. "The attack can be achieved either by encouraging the victim to visit a malicious Web page or placing a script within...an HTML e- mail," the advisory stated. Symantec's Antispam software has a similar issue caused by a different ActiveX component. Fixes for the flaws can be downloaded using Symantec's LiveUpdate.

Category 21.2 Security product QA failures

2004-04-06 software flaw hole vulnerability F-secure patch fix hackers anti-virus rooting owning

DHS IAIP Daily; http://www.vnunet.com/News/1154100

April 06, vnunet.com (UK) — F- Secure warns on software flaw.

Security vendor F- Secure is urging users to patch their systems after the discovery of two flaws in a version of its anti- virus software that leaves users vulnerable to hackers and virus writers. The first flaw could give hackers complete access to a target PC through a hole that affects F- Secure BackWeb 6.31 and earlier versions. This makes the company's anti- virus, BackWeb and policy management software vulnerable. The second problem is in versions 5.41 and 5.42 of F- Secure's Anti- Virus for MIMEsweeper product. It allows the Sober D worm, which is sent in email- attached Zip files, to bypass the antivirus software and infect PCs. Additional information and a patch available here: http://secunia.com/advisories/11297/4/2004

Category 21.2 Security product QA failures

2004-04-22 software vulnerabilities Symantec security products testing

NewsScan

FLAWS FOUND IN SYMANTEC PRODUCTS

The security firm eEye Digital Security has discovered four more critical vulnerabilities in three Symantec products and released basic details about them in its upcoming advisory section, where it maintains a list of flaws its researchers have found in software. As part of its policy of informing the public of upcoming security advisories, eEye normally informs the vendor and then waits for a patch before issuing full details of the flaw in question. The newly reported flaws could result in the execution of remote code. (The Age 22 Apr 2004)

Category 21.2 Security product QA failures

## 2004-05-12 vulnerability Symantec DNS NetBIOS

DHS IAIP Daily; http://www.eweek.com/article2/0,1759,1591455,00.asp

May 12, eWEEK — Multiple vulnerabilities found in Symantec client products.

Symantec has acknowledged several serious bugs in several of its client security products in both corporate and consumer editions. The problems involve several functions of the products but one specific file, SYMDNS.SYS. Fixes for all of the problems are available through Symantec's LiveUpdate and technical- support channels. Products affected include Symantec Client Firewall versions 5.0.0 through 5.1.1; Symantec Client Security 1.0.0, 1.1.0 and 2.0.0; Norton AntiSpam 2004; Norton Internet Security 2002 through 2004; and Norton Internet Security Professional Edition 2002 through 2004. DNS response is one of the functions listed as having such an error. A malicious response to a DNS request could cause the program to fail or alter the flow of the program. There are also errors in the processing of NetBIOS Name Service responses that could allow remote code execution or denial of service. Since NetBIOS is not a routable protocol, such attacks would have to come from within a network segment. Additional information is available on the Symantec Website: http://securityresponse.symantec.com/avcenter/security/Content/2004.05.12.html

Category 21.2 Security product QA failures

2004-08-03 Juniper Network NetScreen firewall vulnerability SSHv1 denial of service

DHS IAIP Daily; http://www.juniper.net/support/security/alerts/screenos- sshv 1- 2.txt

August 03, Juniper Networks — NetScreen DoS Advisory.

The Juniper Networks NetScreen firewall SSHv1 service implementation has a bug which allows an attacker to crash ScreenOS. A malicious person who can connect to the SSHv1 service on a Juniper Networks Netscreen firewall can crash the device before having to authenticate. Upon execution of the attack, the firewall will reboot or hang, which will prevent traffic to flow through the device. Juniper Networks currently has updated versions of ScreenOS available for immediate download.

Category 21.2 Security product QA failures

2004-08-10 Symantec Clientless VPN Gateway vulnerabilities ActiveX browser hotfix available

DHS IAIP Daily; http://secunia.com/advisories/12254/

August 10, Secunia — Symantec Clientless VPN Gateway 4400 Series multiple vulnerabilities.

Multiple vulnerabilities have been reported in Symantec Clientless VPN Gateway 4400 Series, where some have an unknown impact and others can be exploited to conduct cross- site scripting attacks or manipulate users' signon information: 1) Various unspecified vulnerabilities affect the ActiveX and HTML file browsers; 2) Various unspecified input validation errors within the end user UI can be exploited to conduct cross- site scripting attacks; 3) An error within the end user UI can be exploited by malicious users to manipulate other users' signon information (including username and password). A hotfix is available from Symantec: ftp://ftp.symantec.com/public/en..\_5/updates/SCVG5- 20040806- 00.tgz

Category 21.2 Security product QA failures

## 2004-08-25 Cisco Secure Access Control Server ACS vulnerabilities update issued

DHS IAIP Daily;

http://www.cisco.com/warp/public/707/cisco- sa- 20040825- acs.s html

August 25, Cisco Security Advisory — Multiple vulnerabilities in Cisco Secure Access Control Server.

Multiple vulnerabilities exist in Cisco's Secure Access Control Server (ACS) that may cause a crash impacting the availability of services on the ACS devices. The device must be rebooted to resolve this Denial of Service. Other vulnerabilities associated with this advisory may allow unauthenticated users to gain access to the ACS Administration GUI. Updates are available from the vendor at the Source link.

Category 21.2 Security product QA failures

2004-10-05 Symantec Norton Anti-Virus MS DOS device name scan failure update issued

DHS IAIP Daily; http://securityresponse.symantec.com/avcenter/security/Content/2004.10.05.html

October 05, Symantec — Symantec Norton Anti- Virus fails to scan files named with MS DOS device names.

Symantec Norton AntiVirus consumer products do not effectively scan files with MS- DOS reserved device names once the file is resident on a user's system. A remote user can create a file that will not be detected by the application. The vendor has issued a fix for Symantec Norton Anti- Virus 2004, available via LiveUpdate. Fixes for other supported versions will be available through LiveUpdate at a later date.

Category 21.2 Security product QA failures

## 2004-10-18 software anti-virus detection evasion vulnerability

DHS IAIP Daily;

http://www.idefense.com/application/poi/display?id=153&type=vulnerabilities&flashstatus=true

October 18, iDEFENSE — Multiple vendor anti- virus software detection evasion vulnerability.

Remote exploitation of an exceptional condition error in multiple vendors' anti- virus software allows attackers to bypass security protections by evading virus detection. The problem specifically exists in the parsing of .zip archive headers. This vulnerability affects multiple anti- virus vendors including McAfee, Computer Associates, Kaspersky, Sophos, Eset and RAV. See iDEFENSE Advisory in Source link for vendor fixes.

Category 21.2 Security product QA failures

## 2004-11-03 F-secure antivirus Microsoft Exchange mail server ZIP archive malicious code update issued

DHS IAIP Daily; http://securitytracker.com/alerts/2004/Nov/1012057.html

November 03, SecurityTracker — F- Secure Anti- Virus for Microsoft Exchange vulnerability.

A vulnerability was reported in F- Secure Anti- Virus for Microsoft Exchange which could allow a remote user to can send malicious code within a ZIP archive that will pass through the anti- virus function without detection. The vendor reported that some password protected files are not detected inside a ZIP archive. The vendor has released F- Secure Anti- Virus for Microsoft Exchange 6.3x Hotfix 2, available at: ftp://ftp.f- secure.com/support/hotfix/fsav- mse/fsavmse63x- 02.zip

Category 21.2 Security product QA failures

## 2004-12-15 Adobe Acrobat Reader buffer overflow vulnerability code execution attack update issued

DHS IAIP Daily; http://secunia.com/advisories/13474/

December 15, Secunia — Adobe Acrobat Reader "mailListIsPdf()" function buffer overflow.

A vulnerability has been reported in Adobe Acrobat Reader 5.0.9 for Unix, which can be exploited by malicious people to compromise a user's system. The vulnerability is caused due to a boundary error in the "mailListIsPdf()" function when checking input files. This can be exploited to cause a buffer overflow by sending an e- mail with a malicious PDF document attached or a link to one. Successful exploitation allows execution of arbitrary code. Update to version 5.0.10 for Unix: http://www.adobe.com/products/acrobat/readstep2.html

Category 21.2 Security product QA failures

## 2004-12-15 Ethereal network sniffer software vulnerabilities denial of service DoS

DHS IAIP Daily; http://secunia.com/advisories/13471/

December 15, Secunia — Ethereal multiple vulnerabilities.

Multiple vulnerabilities exist which can be exploited by malicious people to cause a DoS (Denial of Service) and potentially compromise a vulnerable system including execution of arbitrary code. Vulnerabilities include errors within the DICOM dissector, the handling of RTP timestamps, the HTTP dissector, and the SMB dissector. Update to version 0.10.8: http://www.ethereal.com/download.html

# Category 21.2 Security product QA failures 2004-12-21 Kerberos V5 authentication software open source buffer overflow vulnerability update issued

DHS IAIP Daily; http://secunia.com/advisories/13592

December 21, Secunia — Kerberos V5 "libkadm5srv" buffer overflow vulnerability.

A vulnerability has been reported in Kerberos V5, which potentially can be exploited by malicious users to compromise a vulnerable system. The vulnerability is caused due to a boundary error in the libkadm5srv administration library within the "add\_to\_history()" function during the password history handling. This can be exploited to cause a heap- based buffer overflow when a principal changes the password and has a certain password history state. The vulnerability is fixed in version 1.4- beta3. The vulnerability will reportedly be fixed in the upcoming krb5- 1.4 release and krb5- 1.3.6 patch release. Apply patch for version 1.3.5: http://web.mit.edu/kerberos/advisories/2004- 004- patch\_1.3.5. txt

## **22.1 DoS attacks**

Category 22.1 DoS attacks

## patch flaw vulnerability fix Sun ONE buffer overflow denial of service DoS

DHS/IAIP Update

2004-01-14

BUFFER OVERFLOW PLUGGED IN SUN ONE WEB SERVER.

Sun Microsystems on Monday, January 12, warned of a buffer overflow vulnerability in its Sun ONE/iPlanet Web Server product. The firm said the flaw could be exploited by a remote user to crash the Web server, which is a type of denial-of-service attack. Independent research firm Secunia has rated the security hole as "moderately critical." The vulnerability affects the Sun ONE/iPlanet Web Server 6.0 Service Pack 5 and earlier versions on the HP-UX platform. Sun has issued a new service pack to fix the flaw, noting that there are no workarounds. The susceptible products are a crucial part of Sun's Web services initiative which falls under Sun Open Net Environment (Sun ONE) brand. The Sun ONE brand includes the Sun ONE Web Server, Sun ONE Portal Server, Sun ONE Application Server, Sun ONE Directory Server, Sun ONE Identity Server, Sun ONE Messaging Server and the Sun ONE Integration Server (all formerly iPlanet products). A service pack is available online: http://wwws.sun.com/software/download/products/3f186391.html

Category 22.1 DoS attacks

## 2004-01-26 computer network vulnerability Internet security

NIPC/DHS; http://news.com.com/2100-7355\_3-5145863.html?tag=nefd\_top

January 22, CNET News.com — Security pros question flaw find.

Two Internet software developers who said they have uncovered a way to cause entire networks of computers to freeze or shut down may have simply rediscovered an old network issue. The network performance issues are described in a series of Web site forum postings recently publicized within the security community. The poster, who uses the alias NT Canuck, said he created a tool, with the help of another developer, that can shut down entire networks. However, security researchers at the Computer Emergency Response Team (CERT) Coordination Center downplayed the issue, saying that the program simply inundates a network with so much data that computers have problems functioning correctly. "We don't see any specific vulnerability being discovered here," said Jason Rafail, an Internet security analyst at the center. According to the Web posts, the programmers found that certain circumstances could be created that would cause a network of computers to freeze, and in some cases fail. The developers contacted Microsoft and the CERT Coordination Center; both organizations confirmed that they were contacted in November. However, Microsoft's Security Response Center (MSRC) has not been able to replicate the discoverers' exact findings, said Stephen Toulouse, senior program manager for the MSRC.

Category 22.1 DoS attacks

## 2004-02-03 denial-of-service DoS attack virus work network SCO MyDoom sco.com

NewsScan

SCO SCRAMBLES TO LAUNCH NEW WEB SITE FOLLOWING ATTACK

SCO Group, which saw its Web site taken out by the MyDoom computer worm, launched a new Web site yesterday (www.thescogroup.com), which will serve as its temporary Web site until the worm's barrage against www.sco.com slacks off. "We expect hundreds of thousands of attacks on www.sco.com because of these viruses. Starting on Feb. 1 and running through Feb. 12, SCO has developed layers of contingency plans to communicate with customers, resellers, developers, partners and shareholders," said the company in a statement. The virulence of the MyDoom worm sent a shudder through the Internet security community. "With such a program you could really take out any major Web site on the Internet," says Raimund Genes, European president of security firm Trend Micro. (Reuters/New York Times 3 Feb 2004)

### DoS attacks Category 22.1 2004-03-19

vulnerability flaw hole patch fix OpenSSL SSL TLS Internet e-commerce security

## DHS IAIP Daily:

March 18, vnunet.com — OpenSSL patches denial of service flaws.

The OpenSSL Project issued patches Wednesday, March 17, to fix two flaws that could leave secure servers open to denial of service (DoS) attacks. An advisory posted on the site warned that both vulnerabilities could allow a remote attacker, using a carefully crafted Secure Sockets Layer (SSL)/Transport Layer Security (TLS) handshake against a server using the OpenSSL library, to cause OpenSSL to crash. Depending on the application this could lead to a DoS. These vulnerabilities have been fixed in OpenSSL 0.9.6m and 0.9.7d, available from the project's Website: http://www.openssl.org/

Category 22.1 DoS attacks

#### 2004-04-19 ColdFusion MX Macromedia denial-of-service DoS vulnerability patch

DHS IAIP Daily; http://www.esecurityplanet.com/trends/article.php/3342061

April 19, eSecurity Planet — ColdFusion MX DoS vulnerability patched.

Graphics design software specialist Macromedia has rolled out a fix for a denial- of- service vulnerability found in its ColdFusion MX 6.1 product suite. The firm said the flaw affected all editions of ColdFusion MX 6.1 and all versions of ColdFusion MX 6.1 J2EE. Macromedia tagged the issue as "important" and recommended that users apply the accompanying patch immediately. ColdFusion MX, formerly known as "Neo," is a key part of Macromedia MX, an integrated collection of tool, server and client technologies developed to function as a single environment. But, security bugs have followed the product around with the latest centering around the way ColdFusion MX handles file uploads. "When file uploads to ColdFusion MX via an HTML form are started, but are interrupted before they complete - disk space on the server may not be reclaimed when the ColdFusion MX template finishes processing," the company explained.

Category 22.1 DoS attacks

#### 2004-06-15 network attack vandalism Websites down denial-of-service Akamai

NewsScan

ATTACK KNOCKS MAJOR SITES OFFLINE

An attack this week by network vandals struck Akamai Technologies, which provides data services for Microsoft, Yahoo, Federal Express, Xerox, the FBI and other major organizations; the attack brought down many of the world's most-visited Web sites for about 45 minutes. An Akamai executive says the company has "no reason to believe that the attack was directed solely at Akamai." The company manages approximately 15% of the traffic on the Internet. (Washington Post 15 Jun 2004)

Category 22.1 DoS attacks

#### 2004-08-24 Symantec security product vulnerabilities denial of service DoS

DHS IAIP Daily; http://secunia.com/advisories/12371/

August 24, Secunia — Symantec multiple products ISAKMPd denial of service vulnerability.

A Denial of Service (DoS) vulnerability exists in multiple Symantec products due to an unspecified error within the isakmpd service. Mulitple platforms are affected for VelociRaptor 1.5, Gateway Security 1.0 and 2.0, and Enterprise Firewall/VPN 7.0 and 7.0.4. Vendor updates are available: http://secunia.com/advisories/12371/

Category 22.1 DoS attacks

#### 2004-08-25 denial-of-service DoS attack Novell Bordermanager VPN service

DHS IAIP Daily; http://www.kb.cert.org/vuls/id/432097

August 25, US- CERT — Vulnerability Note VU#432097: Novell Bordermanager VPN Service denial of service vulnerability.

A Denial of Service (DoS) vulnerability exists in the Novell Bordermanager VPN service that could cause an affected device to crash. The Novell Bordermanager product includes Virtual Private Network (VPN) capabilities, including support for the standard Internet Key Exchange (IKE) protocol. A flaw exists in the way the VPN service handles certain malformed IKE packets which creates a remotely exploitable Denial of Service vulnerability. A vendor solution is available: http://support.novell.com/cgi- bin/search/searchtid.cgi?/1009 3576.htm

## Category 22.1 DoS attacks

## 2004-08-31 WS\_FTP file transfer protocol server application denial of service DoS vulnerability anonymous usage

DHS IAIP Daily; http://secunia.com/advisories/12406/

August 31, Secunia — WS\_FTP server file path parsing denial of service vulnerability.

According to Secunia Advisory SA12406, vulnerability exists in WS\_FTP Server version 5.0.2, which can be exploited by malicious users to cause a DoS (Denial of Service). The problem is caused due to an error in the parsing of file paths and can be exploited to cause a vulnerable system to use a large amount of CPU resources. Successful exploitation requires that the user has been authenticated. There is no vendor solution available at this time. As a workaround, restrict access to the FTP server and disallow anonymous usage.

### Category 22.1 DoS attacks

## 2004-09-02 HP Systems Insight Manager user login denial of service DoS Microsoft security patch update issued

DHS IAIP Daily; http://www.securitytracker.com/alerts/2004/Sep/1011141.html

September 02, SecurityTracker — HP Systems Insight Manager may not let users login after applying a Microsoft security patch.

The Microsoft security fix described in Microsoft security bulletin MS04- 025 prevents users from logging in to HP Systems Insight Manager with Internet Explorer. This issue appears to be more of an incompatibility issue, rather than a security vulnerability. The vendor has issued a fix, available at: http://h18013.www1.hp.com/products/servers/management/hpsim/index.html?jumpid=go/hpsim

Category 22.1 DoS attacks

## 2004-09-06 gnubiff POP3 mail server buffer overflow denial of service DoS vulnerabilities

DHS IAIP Daily; http://secunia.com/advisories/12445/

September 06, Secunia — gnubiff POP3 buffer overflow and denial of service vulnerabilities.

Two vulnerabilities exist in gnubiff, which potentially can be exploited to cause a DoS (Denial of Service) or compromise a vulnerable system. An unspecified boundary error exists within the POP3 functionality. This can be exploited to cause a buffer overflow and may potentially allow execution of arbitrary code. Update to version 2.0.0 or later: http://sourceforge.net/project/showfiles.php?group\_id=94176

Category 22.1 DoS attacks

### 2004-11-05 Symantec LiveUpdate ZIP decompression denial of service DoS no update issued

DHS IAIP Daily; http://securitytracker.com/alerts/2004/Nov/1012095.html

November 05, SecurityTracker — Symantec LiveUpdate zip decompression routine may let users deny service.

The LiveUpdate decompression routine does not check for uncompressed file sizes before attempting to decompress a downloaded LiveUpdate zip file and does not properly validate directory names before creating the directories on the target system. A user can replace a downloaded zip archive (or spoof the Symantec site) and can cause denial of service conditions if the zip archive is crafted to contain an overly large file. There is no solution at this time

# Category 22.1 DoS attacks 2004-11-26 UK government computer failure denial of service DoS Department Work Pensions DWP network

DHS IAIP Daily;

http://www.pcadvisor.co.uk/index.cfm?go=news.view&news=4331

November 26, IDG News Service — UK government hit with another large computer failure.

IT system failures continued to plague the UK government last week, when as many as 80,000 civil servants working for the Department of Work and Pensions (DWP) had to deal with what is being described as the biggest computer crash in government history. The DWP was carrying out a "routine software upgrade" on Monday, November 22, when the system crashed, leaving around 80 percent of the department's 100,000 desk machines disrupted or completely shut down, a DWP spokesperson said Friday, November 26. The problems lasted through most of Thursday, November 25. Microsoft and EDS (Electronic Data Systems) run the DWP's network. The DWP is responsible for providing a variety of state benefits to about 24 million people. It is believed that the crash was caused when an incompatible system was downloaded on to the entire network. The IT failure was only the latest in a string of serious computer system problems experienced by the department.

## 22.4 Accidental availability disruptions

Category	22.4	Accidental availability disruptions		
2004-02-	09	DNS registration e-mail failure denial of service availabilit	у	
RISKS			23	18
*WASHP	OST* REG	ISTRATION EXPIRED, NEWSROOM HAMPERED		
		*The New York Times*, 6 Feb 2004, reported (and not *too* smugly) that s disrupted when registration lapsed for washpost.com, which the newsroo		
was not c		om Network Solutions was delivered unnoticed to a "dropbox" (whether ever, the registration was renewed soon after the disruption started, before a mage.)		
Category	22.4	Accidental availability disruptions		
2004-02-	21	process control sewage hotel Windows complexity availab	ility	
RISKS			23	20
THE BLU	JE SCREEN	N OF SEWAGE		
and "w	vhatever wer	orts in RISKS that a modern hotel found itself without toilets because its N at wrong with it was so obscure that they had to get a technician from the o tland to fix it and reboot." She asks, "The Blue Screen of Sewage?"		
Category	22.4	Accidental availability disruptions		
2004-03-		satellite solar noise availability denial of service outage co StarBand	nmunicatio	ns ISP
RISKS			23	24
THE SUN	N IS VERY	BRIGHT		
communi	cations satel	ustomers of a "sun outage" in the spring and fall of the year when the sun i lites. The blast of intense radiation overpowers the downlink from the sate for a few minutes until the and the geosynchronous satellite move away free	llite to the hon	
Category	22.4	Accidental availability disruptions		
2004-03-		denial-of-service DoS outage Microsoft Hotmail MSN Me	ssenger	

NIPC/DHS

March 14, PC World — Outage hits Hotmail, MSN Messenger.

Internal technical problems at Microsoft closed down access for many MSN Messenger and Hotmail users, as well as some MSN Internet Access customers, for about eight hours Friday, March 12. Microsoft started receiving reports or problems with its instant messaging, Web based e- mail and dial- up Internet services at about 8:30 a.m. Pacific Time Friday, a company spokesperson says. The issue was identified at around 3 p.m. and solved an hour and a half later, she adds. "The outage was pretty significant in terms of the number of customers it affected, but by now the services should be up and running for everybody," the Microsoft spokesperson confirmed late on Friday afternoon. "It was a completely internal issue," the spokesperson says. The problem had nothing to do with hackers or the security patch for MSN Messenger that Microsoft released earlier this week, she adds. Microsoft did not disclose how many customers were unable to connect to those services in the interim. Service complaints came mostly from the U.S. and Canada, but users outside of North America may also have been affected, the spokesperson says. Users who were already connected to the services were for the most part able to continue using them, the issue primarily affected new log- ons, she says.

Category 22.4	Accidental availability disruptions
2004-03-22	denial-of-service DoS outage Microsoft Hotmail MSN Messenger

## NIPC/DHS

March 19, IDG News Service — Hotmail, MSN Messenger hit with another outage.

Technical problems at Microsoft Corp. for the second time within a week caused trouble for users trying to connect to Hotmail and MSN Messenger, the company said Thursday, March 19. Users around the globe reported that they had problems signing on to the Hotmail and MSN Messenger services during about a three- hour period from 5:00 p.m. GMT until 8:00 p.m. GMT Thursday. Microsoft in a statement said it identified an issue that caused log- on and connectivity issues on some MSN services for a portion of its customers and has since solved it. The company did not specify the scope of the problem. The outage also affected connectivity for MSN Internet Access customers, Microsoft said. The company blames the problems on an unspecified internal problem and said it has no indication of any external causes such as cyberattacks. Although to users the problem was essentially the same, Microsoft said that Thursday's problems are different from those that caused an approximately eight- hour outage last Friday.

Category 22.4 Accidental availability disruptions

## 2004-04-26 Internet connectivity lost SBC communications DSL subsriber

DHS IAIP Daily;

http://www.stamfordadvocate.com/news/local/state/hc- 26154805 .apds.m0421.bc- ct- brf- - apr26,0,7979178.story?coll=hc- headlin es- local- wire

April 26, Associated Press — SBC customers cut off from the Internet.

Connecticut customers who use SBC Communications to reach the Internet were cut off from the World Wide Web much of Monday, April 26, after a fiber optic line was cut, the company said. Beverly Levy, an SBC spokesperson, said the outage had cut service to customers who used SBC Dial- up or the DSL broadband service. Levy said that the vendor whose fiber line was cut Monday morning worked around the problem by routing Connecticut Internet traffic through New Jersey. By 3 p.m. customers had service restored, the company said.

## Category 22.4 Accidental availability disruptions

## 2004-05-01 **computer glitch air line testing availability**

DHS IAIP Daily;

http://www.cnn.com/2004/TRAVEL/05/01/delta.delays/index.html

May 01, CNN — Computer glitch grounds Delta flights.

A glitch in a Delta Air Lines computer system grounded flights out of Atlanta on Saturday afternoon, May 1, because data needed for takeoffs was not available, an FAA spokesperson said. Flights in some other cities were affected by the delays. Initially all flights east of Salt Lake City, Utah, were grounded, but within a couple of hours, flights were beginning to take off from airports other than Atlanta, Delta spokesperson Liza Caceres said. By early evening, the delays and cancellations were mostly confined to the Central and Eastern United States, Delta spokesperson Andy McDill said. The Atlanta- based airline uses the computer data in question to calculate weight and balance, and process passenger- related information, said Kathleen Bergen of the FAA. "It's not a safety- related issue," Bergen said.

Category 22.4	Accidental availability disruptions
2004-06-03	confidentiality availability access death posthumous computers documents
	information wills

 $\label{eq:http://www.nytimes.com/2004/06/03/technology/circuits/03data.html?8cir=&pagewanted=print&position=$ 

PUT YOUR PASSWORD IN YOUR WILL?

A growing number of people are storing valuable family information on their computers. Some of them are applying security measures. Unfortunately, many of those people are forgetting to provide appropriate ways of getting into their secured computer systems if they are incapacitated. Other problems once access is gained:

\* embarrassing or otherwise confidential information may be revealed inappropriately;

\* intellectual property such as book manuscripts may not belong to the people who receive the computers;

\* work-related files stored on personal computers may lead to liability for executors if there is a breach of confidentiality;

\* important information may be available through Web accounts but the owners may forget to make the passwords available to families.

Category22.4Accidental availability disruptions2004-12-08interactive games Halo Microsoft Xbox Internet traffic saturation bandwidth

NewsScan; http://news.bbc.co.uk/1/hi/technology/4079397.stm

THE HALO EFFECT: NETWORK GRIDLOCK

The November 9 launch of Microsoft's Halo 2 Xbox game sparked an Internet traffic explosion that has continued into December and could herald chronic network congestion problems for Internet service providers, warns network monitoring firm Sandvine. "The explosion in Xbox Live traffic attributed to Halo 2 should be seen as a clarion call. ISPs need to enhance the broadband experience for these high-end users by prioritizing or reserving bandwidth for games," says Sandvine CTO Marc Morin. One of the main factors that can disrupt online gaming is "lag," in which there is a noticeable delay between the player's action and the game's response time. Installing software that makes networks more "intelligent" will be key to ISPs' ability to accommodate bandwidth-hungry gamers, says a Yankee Group analyst: "In the competitive broadband environment, operators need to differentiate the way they offer access to services like live-play gaming." (BBC News 8 Dec 2004)

## 23.1 Java

Category23.1Java2004-02-23JAVA virtual machine support vulnerability MS Microsoft

RISKS

MICROSOFT DUMPS JAVA VM

23

20

Consultant Ferdinand John Reinke wrote in RISKS: "Are you familiar with the MS Java Virtual Machine (MSJVM) issue? After September 30th 2004, Microsoft will no longer be able to support this technology. As a result, customers who have the MSJVM installed after this date will be vulnerable to potential attacks that will attempt to exploit this technology. This problem is compounded by the fact that Microsoft will no longer be able to provide software updates or patches to the MSJVM. This issue is not just a concern for organizations that use Java, but will also impact anyone who has the MSJVM installed. More alarming, many organizations aren't even aware that they have MSJVM installed."

Later, in RISKS 23.23, Jonathan de Boyne Pollard suggested that the change of support would have no immediate effects: "The software is not, after all, magically changing somehow on that date to become more vulnerable." He also denied that the security implications of awareness of what software one has on one's system is in any way related to whether the software is supported or not.

[MK comments: The issue is whether anyone is going to provide patches, and if so, how quickly. As for knowing what one has on one's system, it's very unlikely that a system manager will patch what (s)he doesn't know is being used on the system.]

Category 23.1 Java

## 2004-10-08 Java Sun Eastman Kodak patent

NewsScan; http://australianit.news.com.au/articles/0

SUN SETTLES JAVA SUIT FOR \$92 MILLION

Eastman Kodak has accepted a \$92-million offer by Sun Microsystems to settle a billion-dollar patent-infringement lawsuit over the Java programming language. A U.S. federal jury decided last Friday, after a three-week trial, that Java infringed on patents Kodak acquired when it bought Wang Laboratories' imaging software business for \$260 million in 1997. The night before the trial's damages phase, which was to begin Thursday, the companies ended their two-year-old battle in an out-of-court settlement. Without admitting or denying the allegations, Sun Microsystems said it will pay Kodak \$92 million to settle all claims in the dispute. In exchange, Sun received a license for Java under all Kodak patents. (The Australian, 8 Oct 2004)

Category 23.1 Java

## 2004-11-01 Sun Java Web Proxy Server buffer overflow vulnerability denial of service DoS update issued

DHS IAIP Daily; http://secunia.com/advisories/13036/

November 01, Secunia — Sun Java System Web Proxy Server unspecified buffer overflow vulnerabilities.

Some vulnerabilities have been reported in Sun Java System Web Proxy Server 3.6 Service Pack 4 and prior. These vulnerabilities can be exploited by malicious people to cause a DoS (Denial of Service) or compromise a vulnerable system. The vulnerabilities are caused due to some unspecified boundary errors that can be exploited to cause buffer overflows. Apply Service Pack 5 or later: http://wwws.sun.com/software/download/products/4149bc42.html

Category 23.1 Java

## 2004-12-20 Google Desktop Search local search integration result disclosure remote Java applet exploit update issued

DHS IAIP Daily; http://securitytracker.com/alerts/2004/Dec/1012624.html

December 20, SecurityTracker — Google Desktop Search discloses local search integration results to remote users.

A remote user can create a Java applet that, when loaded by the target user, will execute queries to the remote server that served the Java applet that appear to the Google Desktop Search application to be valid Google queries, causing the search application to integrate the local search results with the information returned by the remote server that served the Java applet. The applet running on the target user's system will then have access to the integrated local search results and can forward those results to the remote server. The vendor has released a fixed version (121004) as of December 10, 2004.

## 23.2 Javascript

Category 23.2 Javascript

2004-08-03

## Mozilla Netscape browser critical flaw vulnerability Javascript Webpages

DHS IAIP Daily; http://www.internetnews.com/security/article.php/3389941

August 03, internetnews.com — PC takeover flaw in Mozilla, Netscape.

Security researchers have discovered a "highly critical" security hole in the Netscape and Mozilla browsers that puts users at risk of computer takeover. According to an advisory from iDefense, the vulnerability is caused by an integer overflow within the SOAPParameter object's constructor. SOAPParameter objects handle support for SOAP, the XML- based messaging protocol that defines rules for structuring messages. "Successful exploitation allows the remote attacker to execute arbitrary code in the context of the user running the browser," iDefense warned. The flaw can be exploited via specially created Web pages containing malicious Javascript. Browser products affected include Mozilla 1.6; and Netscape versions 7.0 and 7.1. The research firm recommends that Netscape users disable Javascript in the browser as a workaround. The open- source Mozilla Foundation has released an update to fix the flaw: http://www.mozilla.org/products/mozilla1.x/

Category 23.2 Javascript

2004-12-08 multiple browser injection vulnerability JavaScript exploit no update issued

DHS IAIP Daily; http://www.securitytracker.com/archives/summary/9000.html

December 08, SecurityTracker — Multiple browsers window injection vulnerability.

A remote user can inject arbitrary content into an open window in certain cases to spoof Website contents. It is reported that if the target name of an open window is known, a remote user can create Javascript that, when loaded by the target user, will display arbitrary content in the opened window. A remote user can exploit this to spoof the content of potentially trusted Websites. Specific browsers affected are Apple Safari, KDE Konqueror, Microsoft Internet Explorer, Mozilla Firefox, Netscape, and Opera. There is no solution at this time.

## 23.4 HTML, XML

Category 23.4 HTML, XML

## W3C Web DARPA standards adoption Defense Research Projects Agency

DHS IAIP Daily;

2004-02-18

http://fcw.com/fcw/articles/2004/0216/web- daml- 02- 19- 04.asp

February 18, Federal Computer Week — W3C adopts DARPA language.

The Defense Advanced Research Projects Agency (DARPA) this month announced that the World Wide Web Consortium (W3C) approved a computer language based on DARPA Agent Markup Language (DAML) as an international standard. Web Ontology Language, known as OWL, was designated an official Web standard, joining such better- known languages as HTML and Extensible Markup Language (XML). The DARPA markup language project last year evolved into OWL and is continuing development under W3C's watch. OWL builds on XML and is designed to allow a higher level of interoperability among devices, Web sites and databases. It uses XML as to transport data, but OWL is designed to link disparate data from different sources and determine relationships between them. OWL's proponents say it can refine searches and Web services, giving users more accurate and precise information based on queries. And the language could potentially let computers recognize how disparate forms of information are linked and draw conclusions based on those links.

Category 23.4 HTML, XML

### XML Extensible Markup Language security concern

2004-03-20 NIPC/DHS

March 29, CNET News.com — Extra headaches of securing XML.

Extensible Markup Language and XML- based protocols are rapidly becoming a common way for businesses to format and exchange corporate information. Businesses typically have used Web services to connect internal applications and share information with a well- known network of business partners. However, once companies start using Web services and XML more extensively, they need to reconsider how they are exposing their data- - and to what, Gartner analyst Benoit Lheureux said. Infiltrating a corporate network by tapping into Web services interfaces is potentially more damaging than simply knocking out a Website, because business- to- business applications expose valuable corporate information, he noted. Typical security products are designed to keep unwanted intruders from entering corporate networks or to prevent attacks that can disable a machine. Applications that send information via XML documents use the same Internet network protocols that traditional security products monitor. But because XML messages are wrapped in the IP "envelope" that most firewalls are designed to track, corporate networks inspect the envelope but not the contents. Fraudulent XML messages could therefore enter corporate networks undetected.

Category 23.4 HTML, XML

### 2004-07-30 Microsoft security bulletin patch update privilege US-CERT

DHS IAIP Daily;

http://www.microsoft.com/technet/security/bulletin/ms04-025.mspx

July 30, Microsoft — Microsoft Security Bulletin MS04- 025: Cumulative Security Update for Internet Explorer.

This update resolves several newly discovered public vulnerabilities. If a user is logged on with administrative privileges, an attacker who successfully exploited the most severe of these vulnerabilities could take complete control of an affected system, including installing programs; viewing, changing, or deleting data; or creating new accounts with full privileges. Users whose accounts are configured to have fewer privileges on the system would be at less risk than users who operate with administrative privileges. Microsoft has assigned a risk rating of "Critical" to this issue and recommends that users install the patch immediately. US- CERT released Technical Cyber Security Alert TA04- 212A: Critical Vulnerabilities in Microsoft Windows for this issue: http://www.us- cert.gov/cas/techalerts/TA04- 212A.html

## Category23.4HTML, XML2004-10-04XML RSS Really Simple Syndication broadcasting

NewsScan; http://online.wsj.com/article/0

RSS GIVES XML A NEW LEASE ON LIFE

A year ago, blogs were widely regarded as the private diaries of tech-savvy eccentrics, and pundits were still waiting for the highly touted XML (extensible markup language) to make its mark on the Net, says Wall Street Journal columnist Lee Gomes. "Fast forward now to something called RSS, or Really Simple Syndication, which is a technology that bloggers use to, in a manner of speaking, broadcast their writing throughout the Internet. RSS, it turns out, is actually a kind of XML... In other words, thanks to blogs, XML -- in the form of RSS -- has finally arrived. This real XML revolution, though, is nothing like the stolid, corporate, rather dull affair that was first predicted. (If you liked database algorithms, you'd have loved XML.) Instead, it has a grassroots, quirky, somewhat antiauthoritarian cast to it." Gomes warns that while some major Internet giants, such as Yahoo and Microsoft, have signed on to support RSS feeds, blogs may ultimately change the traditional Web economics, because readers can skip frequent visits to their sites to check for new content. And while most RSS boosters describe the technology as an antidote for information overload, it could make things worse: "As e-mail proves, if it's easy for people to use computers to say something, they will. Do they have something to say? Who cares!" says Gomes.

# 23.5 E-mail & instant messaging or chat

Category 23.5 E-mail & instant messaging or chat

## 2004-01-14 Microsoft security bulletin patch flaw vulnerability fix Exchange Server

NIPC/DHS;

http://www.microsoft.com/technet/treeview/default.asp?url=/technet/security/b ulletin/MS04- 002.asp

January 13, Microsoft — Microsoft Security Bulletin MS04-002: Vulnerability in Exchange Server 2003 Could Lead to Privilege Escalation.

A vulnerability exists in the way that Hypertext Transfer Protocol (HTTP) connections are reused when NTLM authentication is used between front-end Exchange 2003 servers providing Outlook Web Access (OWA) and, OWA on Windows 2000 and Windows Server 2003, and when using back-end Exchange 2003 servers that are running Windows Server 2003. Users who access their mailboxes through an Exchange 2003 front-end server and OWA might get connected to another user's mailbox if that other mailbox is (1) hosted on the same back-end mailbox server and (2) if that mailbox has been recently accessed by its owner. Attackers seeking to exploit this vulnerability could not predict which mailbox they might become connected to. The vulnerability causes random and unreliable access to mailboxes and is specifically limited to mailboxes that have recently been accessed through OWA. This vulnerability is exposed if the Website that is running the Exchange Server 2003 programs on the Exchange back-end server has been configured not to negotiate Kerberos authentication, causing OWA to fall back to using NTLM authentication. The only known way that this vulnerability can be exposed is by a change in the default configuration of Internet Information Services 6.0 on the Exchange back-end server. Microsoft has assigned a severity rating of "Moderate" to this issue.

Category	23.5	E-mail & instant messaging or chat		
2004-01-	28	virus scanners attachment creation update macros conspiracy t	theory	
RISKS			23	15ff
RISKS O	F VIRUS SCAI	NNERS AND MACRO-ENABLED DOCUMENTS		
C D II	1			

Steve Bellovin writes about his experience upgrading AV software. This AV software product dealt with an e-mail with a viral attachment "in an appropriate permanent fashion." However, Bellovin says, the AV software notified the user of its disinfection with a text file attachment to the previously-infected e-mail. Bellovin thinks it won't be long before a virus mimics this AV software's action, to fool a user into opening a "notification" file. He asks, "Why are the good guys trying to teach people to click on attachments?" In a follow-up article, contributor Paul Tomblin answers this question--Tomblin thinks anti-virus companies need people to click on attachments and get infected in order stay in business. In another follow-up article, Alan J Rosenthal argues that "opening "attachments" is a fact of ms-win life." He says that users have become used to sending each other plain text messages as Word document attachments--which may often be infected--and transmitting malicious code through Word macros. Rosenthal thinks this problem could be solved if Microsoft created an Office suite without macros. This way, he says, users won't be able to transmit malicious code so easily, and "everyone else will be impressed by Microsoft's technical mastery..."

Category 23.5 E-mail & instant messaging or chat

2004-03-10 Microsoft security bulletin vulnerability hole flaw patch fix MSN Messenger privacy

DHS IAIP Daily; http://www.microsoft.com/technet/security/bulletin/ms04-010.mspx

March 09, Microsoft — Microsoft Security Bulletin MS04- 010:

Vulnerability in MSN Messenger Could Allow Information Disclosure. A security vulnerability exists in Microsoft MSN Messenger. The vulnerability exists because of the method used by MSN Messenger to handle a file request. An attacker could exploit this vulnerability by sending a specially crafted request to a user running MSN Messenger. If exploited successfully, the attacker could view the contents of a file on the hard drive without the user's knowledge as long as the attacker knew the location of the file and the user had read access to the file. To exploit this vulnerability, an attacker would have to know the sign- on name of the MSN Messenger user in order to send the request. Microsoft has assigned a risk rating of "Moderate" to this issue and recommends that system administrators consider installing the security update.

## Category23.5E-mail & instant messaging or chat2004-03-10Microsoft security bulletin vulnerability hole flaw patch fix Outlook HTML e-mail

## DHS IAIP Daily:

http://www.microsoft.com/technet/security/bulletin/ms04-009.mspx

March 09, Microsoft — Microsoft Security Bulletin MS04- 009: Vulnerability in Microsoft Outlook Could Allow Code Execution.

A vulnerability in Outlook 2002 caused by the parsing of specially crafted mailto URLs exists could allow Internet Explorer to execute script code in the Local Machine zone on an affected system. To exploit this vulnerability, an attacker would have to host a malicious Website that contained a Web page designed to exploit the vulnerability and then persuade a user to view the Web page. The attacker could also create an HTML e- mail message designed to exploit the vulnerability and persuade the user to view the HTML e- mail message. After the user has visited the malicious Website or viewed the malicious HTML e- mail message an attacker who successfully exploited this vulnerability could access files on a user's system or run arbitrary code on a user's system. This code would run in the security context of the currently logged- on user. Microsoft has assigned a risk rating of "Important" to this issue and recommends that system administrators install the patch immediately.

Category 23.5	E-mail & instant messaging or chat
2004-03-12	Microsoft security vulnerability hole flaw patch fix Outlook e-mail

DHS IAIP Daily;

http://www.computerworld.com/securitytopics/security/story/0,10801,90992,00.html

March 10, IDG News Service — Microsoft upgrades fix for Outlook from 'important' to 'critical'.

One day after releasing a trio of security patches, Microsoft is upgrading the seriousness of one of those fixes to from "important" to "critical." The update released in security bulletin MS04- 009 fixes a problem with the way the Outlook e- mail software treats URLs that use the "mailto" tag, which allows Website authors to insert links on Web pages that launch Outlook or other e- mail clients. A problem with the way Outlook interprets mailto URLs could allow an attacker to use a specially formatted mailto URL to gain access to files on an affected system or insert and run malicious computer code. Microsoft initially claimed that only computers with the Outlook Today home page were vulnerable to attack. Outlook Today is the home page only until an e- mail account is created, Microsoft said. However, following release of the bulletin, Finnish security researcher Jouko Pynnonen, who discovered the vulnerability, informed the company that malicious hackers could attack vulnerable Outlook installations even if Outlook Today isn't the default home page, the company said. In a revised version of its security bulletin, Microsoft noted the discrepancy. Additional information is available on the Microsoft Website: http://www.microsoft.com/technet/security/bulletin/offmar04. mspx

# Category 23.5 E-mail & instant messaging or chat 2004-03-24 security vulnerability flaw hole patch fix Web-based electronic e-mail service Hotmail Yahoo

DHS IAIP Daily; http://www.esecurityplanet.com/trends/article.php/3329821

March 23, eSecurity Planet — Hotmail, Yahoo users at risk of PC takeover.

A potentially serious security flaw found in Web- based e- mail services offered by Microsoft and Yahoo could put millions of PCs at risk of takeover, an Internet security consultant GreyMagic warned Tuesday, March 23. The advisory warned that attackers could inject malicious code by simply sending an e- mail to an unsuspecting Hotmail or Yahoo user. The vulnerability only affects Hotmail and Yahoo running on Microsoft's Internet Explorer (IE) browser. Successful exploit could lead to theft of a user's login and password, disclosure of the content of any e- mail in the mailbox and disclosure of all contacts within the address book. Additionally, the attacker could manipulate the system to automatically send e- mails from the mailbox and to exploit vulnerabilities in IE to access the user's file system and eventually take over his or her machine. Microsoft has fixed the vulnerability and Hotmail is no longer vulnerable.

Category 23.5	E-mail & instant messaging or chat
2004-03-26	intant messenging IM threat CERT CC social engineering spam virus back door
NIDC /DUC	

## NIPC/DHS

March 25, New York Times — When instant messages come bearing malice.

Perpetrators are using Instant Messenging (IM) to deliver spam, unleash viruses, and create back doors into the systems of unsuspecting users. The CERT Coordination Center says IM users are especially susceptible to "social engineering," meaning attacks that prey on human foibles by enticing people with promises of free products, pornography and interesting- sounding links. When two people communicate through instant messaging, the messages are relayed as plain text through an IM service's central servers before they reach the recipient. An unscrupulous systems administrator could easily train a program to search for words, passwords or combinations of numbers to harvest critical personal information. The lack of privacy is compounded when IM messages travel over public wireless networks like those at cafes, airports and hotels where security levels are kept low to give users easy access to the network. IM users can transfer files to each other and give others access to their shared- files folder. These folders sometimes contain family photographs and documents with names, addresses and telltale financial information, "all the little pieces of information that actually might help someone assume a person's identity," said Fred Felman of Zone Labs.

Category 23.5 E-mail & instant messaging or chat

## 2004-04-13 Micrsoft security bulletin update Windows critical Outlook e-mail client

DHS IAIP Daily;

http://www.microsoft.com/technet/security/bulletin/ms04-013.mspx

April 13, Microsoft — Microsoft Security Bulletin MS04- 013 Cumulative Security Update for Outlook Express.

This is a cumulative update that includes the functionality of all the previously- released updates for Outlook Express 5.5 and Outlook Express 6. Additionally, it eliminates a new vulnerability that could allow an attacker who successfully exploited this vulnerability to access files and to take complete control of the affected system. This could occur even if Outlook Express is not used as the default e- mail reader on the system. Microsoft has assigned a risk rating of "Critical" to this issue and recommends that customers install this update immediately.

### Category 23.5 E-mail & instant messaging or chat

### 2004-04-27 new e-mail attack denial-of-service servers NDN flooding spoofed addresses

DHS IAIP Daily; http://searchsecurity.techtarget.com/originalContent/0,28914 2,sid14\_gci961512,00.html

April 27, SearchSecurity.com — E- mail attack could swamp e- mail servers.

Several researchers have identified a new e- mail attack that can be used to swamp enterprise e- mail servers, as well as some secondary systems. Experiments revealed that nearly 60% of general and 30% of Fortune 500 systems and domains could be leveraged for an attack. Security consultant Stefan Frei, who operates a Swiss e- mail portal, discovered a way that malicious users could swamp e- mail servers and accounts. In early April he reported it in a paper coauthored with software architect Ivo Silvestri and professional services director Gunter Ollmann. In the report, the trio explained how an attack could happen, beginning with a spoofed e- mail originator at the target. A message is sent to multiple invalid recipients. The system sends NDNs flooding back to the spoofed address. The assault can be further multiplied by adding an attachment to the initial message. The researchers recommend mail server changes to lessen the problem- - such as not accepting mail for invalid recipients, limiting the maximum number of recipients, generating few and small error messages and validating input data. All of these fixes don't help a target ward off an attack. As Ollmann pointed out, about the only option is to block systems at the ISP level by, perhaps, blacklisting offending mail servers.

Category 23.5 E-mail & instant messaging or chat

2004-05-07 buffer overflow vulnerability Eudora e-mail email

DHS IAIP Daily; http://www.esecurityplanet.com/prevention/article.php/335117

May 07, eSecurity Planet — 'Critical' buffer overflow found in Eudora.

Security researchers have discovered a "highly critical" security flaw in QUALCOMM's Eudora e- mail client that could lead to the execution of malicious code on vulnerable systems. Paul Szabo, a computer systems officer at the University of Sydney, reported the flaws in versions 6.1, 6.0.3 and 5.2.1 of Eudora and warned that Windows users were at risk of complete system takeover. According to Szabo's advisory, the vulnerability is due to a boundary error within the URL- handling functionality. A malicious hacker could exploit the hole with an e- mail containing a specially crafted link. Research firm Secunia has tagged a "highly critical" rating on the flaw and recommends that Eudora users be wary of other serious vulnerabilities in the mail client.

Category 23.5 E-mail & instant messaging or chat

## 2004-05-18 vulnerability Microsoft Outlook e-mail client illegal actions update issued

DHS IAIP Daily; http://news.earthweb.com/ent- news/article.php/3355411

May 18, earthwebnews.com — Outlook 2003 bypass flaw reported.

Security researchers have discovered a vulnerability in the Microsoft Outlook 2003 software that could allow malicious hackers to perform illegal actions through e- mails. According to an alert from Secunia, the flaw could let attackers sneak past the security settings in the Outlook 2003 e- mail program and attempt to load harmful code to vulnerable PCs. Outlook 2003 is designed to protect the user by opening mails in a restricted security zone to prevent the use of active scripting or download of harmful files. This can be exploited to start a download sequence of arbitrary files, which in turn causes Internet Explorer to prompt the user whether to download the file," according to the alert, which carries a "moderately critical" rating. Combined with another flaw that deals with "Predictable File Location Weakness," Secunia said it was possible to launch the malicious file without any warning. Affected software include Outlook 2003, Office 2003 Student and Teacher Edition, Office 2003 Standard Edition, Office 2003 Small Business Edition and Office 2003 Professional Edition. The company recommends that users filter HTML and Rich Text Format messages until a fix is issued by the software giant. Alert found at http://secunia.com/advisories/11629/

Category 23.5 E-mail & instant messaging or chat

2004-06-03 e-mail makeover instant messaging IM RSS features

NewsScan

E-MAIL NEEDS A MAKEOVER

Forget about spam -- even your "wanted" e-mail is clogging your in-box now, right? E-mail is "broken," says Eric Hahn, former CTO of Netscape and current CEO of antispam firm Proofpoint. "We need to make metaphoric changes. The [file-folder] metaphor was designed back when we were talking about getting five messages a day." Today, many folks receive 10 to 20 times that number and filing each one just takes too much time. "People hate filing. They hate it in paper. They hate it in e-mail. Could you imagine what it would be like to have to file Web pages just to get

back to them?" Hahn suggests that in addition to overhauling the filing function, software developers should find a way to combine instant-messaging software with e-mail software. "Doesn't it seem odd that IM is separate from e-mail? Why are those conversations so fundamentally

different?" he asks. Ben Gross, a researcher at the University of Illinois-Urbana-Champaign, says that in addition to incorporating IM, e-mail software developers need to integrate RSS readers into their products, so that users can view updates to a Web page without having to download the whole Web page into a browser. Some e-mail software developers are already experimenting with new approaches: Microsoft's Outlook 2003 and Google's Gmail service include a "group by conversation" feature that enables users to view related e-mails sent to and from a single person. (Wired.com 3 Jun 2004)

Category 23.5	E-mail & instant messaging or chat
2004-06-14	e-mail security threat early warning Internet traffic virus worm
NT O	

NewsScan

## E-MAIL SECURITY FIRMS FOCUS ON EARLY WARNING

E-mail security companies are using a new technique to monitor Internet traffic that will allow them to identify virus outbreaks earlier and take a more proactive role in preventing hacker damage. The technology surveys traffic across a large number of organizations and searches for anomalies that might indicate malicious code activity. It then takes immediate action to slow down or block delivery, providing a head-start over conventional methods that analyze viruses and then rely on antivirus firms to identify and stop them. "We've seen we can gain four or five hours on the virus," says Scott Weiss, CEO of IronPort, which uses the early-warning technology. "Four to five hours is life for the network administrator." Suspicious traffic patterns that might signal viral outbreak include an increased volume in messages from specific senders and messages with similar subject lines or containing a particular type of attachment file. The computers can then tip off e-mail software to destroy or quarantine the suspect messages. "It's the start of a big trend," predicts Matt Cain, an analyst with Meta Group. (Wall Street Journal 14 Jun 2004)

Category 23.5	E-mail & instant messaging or chat
2004-06-28	Verisign e-mail security service blacklists identification authentication I&A

NewsScan

VERISIGN TACKLES E-MAIL SECURITY

VeriSign has unveiled a new e-mail protection service that uses custom blacklists, fingerprinting and heuristic tools to calculate the probability that a particular message is spam by examining a pattern of characteristics in the message. The company has begun free trials of the service, and VeriSign says it plans to add more features, including sender ID verification and domain authentication. "The introduction of this service will help enterprises restore the productivity gains from e-mail communication that are now under threat from spam and viruses," says VeriSign executive VP Judy Lin. (CNet News.com 28 Jun 2004)

Category 23.5 E-mail & instant messaging or chat

2004-07-14 e-mail privacy management policy Electronic Frontier Foundation EFF complaint

NewsScan

E-MAIL PRIVACY: DON'T COUNT ON IT

A recent federal appeals court ruling giving e-mail less protection than other types of communication has inspired privacy advocates to reemphasize the need for caution in the use and management of e-mail. Kevin Bankston of the Electronic Frontier Foundation warns: "Under this decision, any node on the Internet that passes e-mails could flip a switch and start looking at any e-mail that passed through it," and Marc Rotenberg of the Electronic Privacy Information Center says that until Congress or the courts change the law "the best practice is not to put into e-mail something that you are concerned might be disclosed to a third party." And privacy expert J.J. Luna gives this piece of good advice: "Never sell a computer with a hard drive to anyone, for any reason." (Wall Street Journal 14 Jul 2004)

Category 23.5 E-mail & instant messaging or chat

### 2004-08-09 AOL Instant Messenger IM critical vulnerability buffer overflow attack

DHS IAIP Daily; http://searchsecurity.techtarget.com/originalContent/0,28914 2,sid14\_gci999090,00.html

August 09, SearchSecurity.com — 'Highly critical' flaw in AOL Instant Messenger.

AOL Instant Messenger (AIM) has a vulnerability attackers could use to compromise computers and launch arbitrary code, IT security firm Secunia said Monday, August 9. AIM 5.x contains a boundary error within the handling of "Away" messages that can be exploited to cause a stack- based buffer overflow. "A malicious Website can exploit this via the AIM URI handler by passing an overly long argument to the 'goaway?message' parameter," the advisory said. "Successful exploitation may allow execution of arbitrary code on a user's system when...a malicious Website is visited with certain browsers." Secunia said the vulnerability has been confirmed in version 5.5.3595 and that other versions may also be affected. The firm also noted that "various other issues were also reported, where a large amount of resources can be consumed on a user's system." The advisory said the vendor was contacted but has not responded, and recommends users switch to an alternative product.

Category 23.5 E-mail & instant messaging or chat

2004-08-13 Yahoo Messenger Portable Network Graphics PNG libpng vulnerability plug

DHS IAIP Daily; http://www.eweek.com/article2/0,1759,1635855,00.asp

August 13, eWEEK — Yahoo plugs PNG security hole.

Yahoo Inc. has posted a security update for its Windows version of Yahoo Messenger to fix a series of vulnerabilities in the PNG (portable network graphics) library, or libpng. The library provides a set of graphics routines for PNG files; PNG is an alternative graphics format to GIF. The PNG library holes, as previously reported, could allow an attacker to crash programs or execute attack code. Yahoo released the fix for users of Yahoo Messenger 6.0 for Windows because it uses the open- source PNG format in limited areas of its IM client to display images, said Yahoo spokesperson Terrell Karlsten. According to a security note on the Yahoo Messenger Website, there have been no known exploits of the vulnerabilities. Yahoo learned of the PNG library vulnerabilities from a U.S. Computer Emergency Readiness Team security bulletin issued last week. Additional information is available on the Yahoo Website: http://messenger.yahoo.com/security/update5.html

Category 23.5 E-mail & instant messaging or chat

## 2004-08-19 Mutt e-mail client PGP GnuPG vulnerability spoof messages social engineering attacks

DHS IAIP Daily; http://www.securityfocus.com/bid/10929

August 19, SecurityFocus — Mutt PGP/GnuPG verified e- mail signature spoofing vulnerability.

Mutt PGP/GnuPG versions 1.3.28 and 1.5.6 contain a vulnerability that allows malicious users to send e- mail that spoofs a successfully verified PGP/GnuPG e- mail message. If a user employs Mutt with a specific configuration, this vulnerability could allow a malicious user to spoof e- mail from trusted sources. This will likely increase the effectiveness of social engineering attacks. Altering the configuration of Mutt to use colors may assist in determining if e- mail messages are spoofed.

Category 23.5 E-mail & instant messaging or chat

### 2004-08-28 Gaim instant messaging client software vulnerabilities

DHS IAIP Daily; http://www.zone- h.org/advisories/read/id=5443

August 28, Zone- H.org - New Gaim vulnerabilities reported.

Gaim contains several security issues that might allow an attacker to execute arbitrary code or commands. Gaim fails to do proper bounds checking under various circumstances. These vulnerabilites could allow an attacker to crash Gaim or execute arbitrary code or commands with the permissions of the user running Gaim. Upgrade to the latest edition of Gaim: http://gaim.sourceforge.net/downloads.php

Category 23.5 E-mail & instant messaging or chat

2004-09-08 Trillian instant messaging IM client MSN module buffer overflow vulnerability no update issued

DHS IAIP Daily; http://secunia.com/advisories/12487/

September 08, Secunia — Trillian MSN module buffer overflow vulnerability.

A vulnerability exists in Trillian 0.74i, which can be exploited by malicious people to execute arbitrary code on a compromised system. Trillian is a chat client currently supporting IRC, AIM, ICQ, MSN Messenger, and Yahoo! Messenger. There is no solution available at this time.

Category 23.5 E-mail & instant messaging or chat

## 2004-09-29 instant messaging IM worm JPEG flaw

DHS IAIP Daily; http://security.itworld.com/4340/040929imworm/page\_1.html

September 29, IDG News Service — Instant messaging worm exploits JPEG flaw.

Security experts have spotted the first attempts to create an Internet worm that propagates using instant messages. Researchers at The SANS Institute's Internet Storm Center (ISC) have had two reports of users receiving messages on America Online Inc.'s Instant Messenger service that lured them to Websites containing malicious code, said Johannes Ullrich, chief technology officer at ISC, on Wednesday, September 29. The malicious code attempts to install "backdoor" software on the user's PC that gives remote attackers control over the machine and the victim's instant messenger contacts list, Ullrich said.

Category 23.5 E-mail & instant messaging or chat

## 2004-11-16 Imail IMAP service buffer overflow vulnerability code execution attack

DHS IAIP Daily; http://secunia.com/advisories/13200/

November 16, Secunia — Imail IMAP service delete command buffer overflow vulnerability.

A vulnerability has been reported in IMail Server, which can be exploited by malicious users to compromise a vulnerable system. The vulnerability can be exploited to cause a stack- based buffer overflow by passing a "DELETE" command with an overly long argument (about 300 bytes). Successful exploitation allows execution of arbitrary code. No vendor solution is available.

Category	23.5	E-mail & instant messaging or chat
----------	------	------------------------------------

## 2004-11-20 Google Gmail zx variable remote user cross site scripting attack vulnerability

DHS IAIP Daily; http://www.securitytracker.com/alerts/2004/Nov/1012289.html

November 20, SecurityTracker — Gmail 'zx' variable input validation bug lets remote users conduct cross- site scripting attacks.

A remote user can access the target user's cookies (including authentication cookies), if any, associated with the Gmail site, access data recently submitted by the target user via Web form to the site, or take actions on the site acting as the target user. It is reported that the zx variable is not properly validated. A remote user can create a specially crafted URL that, when loaded by a target user, will cause arbitrary scripting code to be executed by the target user's browser. From SecurityTracker's testing, it appears that this flaw has been corrected, but that was not confirmed in the report.

## Category23.5E-mail & instant messaging or chat2004-11-29instant messaging IM logging storage retrieval archiving

NewsScan; http://www.siliconvalley.com/mld/siliconvalley/10293868.htm

SMARTER IM-ING

Now there's a new service called IM Smarter that stores copies of conversations for later retrieval, a feature that could become quite handy as instant messaging makes inroads into the corporate world. Inventor David Weekly characterizes IM Smarter as an electronic "secretary" that takes notes and alerts you to important events. "The logging will appeal to people who passed notes in school and would keep them in a shoe box. And there are people who use IM for business purposes and want to keep those conversations." IM Smarter's storage capabilities lend fuel to an emerging debate over how ephemeral instant message conversations should be. Many IM-ers assume their conversations disappear when they (and their correspondents) log off. The IM Smarter service is currently free, but Weekly hopes to add advertising to support it, and eventually launch an ad-free premium service that allows users to set up IM alerts for tracking changes to Web sites or eBay auctions. (San Jose Mercury News 29 Nov 2004)

Category 23.5 E-mail & instant messaging or chat

2004-12-08 Internet security instant messaging IM peer-to-peer virus worm threat tracking

DHS IAIP Daily; http://www.computerweekly.com/articles/article.asp?liArticle ID=135694&liArticleTypeID=1&liCategoryID=6&liChannelID=22&li FlavourID=1&sSearch=&nPage=1

December 08, ComputerWeekly — Group formed to track IM threats.

A group of Internet security and instant messaging (IM) providers have teamed up to detect and thwart the growing threat of IM and P2P (peer- to- peer) viruses and worms. The consortium, led by corporate IM software suppliers, is setting up a threat center to analyze and warn against the vulnerabilities. It is offering free alerts and e- mail notifications of risk assessments and threat management for subscribers. The group's formation follows evidence that security threats against IM and P2P networks are growing. The group includes Imlogic, McAfee, Sybari Software, Yahoo, America Online and Microsoft. The effort is being co- ordinated at the IMlogic Threat Center at http://www.imlogic.com/im\_threat\_center/index.asp

## 23.6 Web-site infrastructure, general Web security issues

Category 23.6 Web-site infrastructure, general Web security issues

## 2004-01-14 patch flaw vulnerability fix Sun ONE buffer overflow

NIPC/DHS; http://www.esecurityplanet.com/prodser/article.php/3298031

January 12, esecurityplanet.com — Buffer overflow plugged in Sun ONE web server.

Sun Microsystems on Monday, January 12, warned of a buffer overflow vulnerability in its Sun ONE/iPlanet Web Server product. The firm said the flaw could be exploited by a remote user to crash the Web server, which is a type of denial-of-service attack. Independent research firm Secunia has rated the security hole as "moderately critical." The vulnerability affects the Sun ONE/iPlanet Web Server 6.0 Service Pack 5 and earlier versions on the HP-UX platform. Sun has issued a new service pack to fix the flaw, noting that there are no workarounds. The susceptible products are a crucial part of Sun's Web services initiative which falls under Sun Open Net Environment (Sun ONE) brand. The Sun ONE brand includes the Sun ONE Web Server, Sun ONE Portal Server, Sun ONE Application Server, Sun ONE Directory Server, Sun ONE Identity Server, Sun ONE Messaging Server and the Sun ONE Integration Server (all formerly iPlanet products). A service pack is available online: http://wwws.sun.com/software/download/products/3f186391.html

Category 23.6 Web-site infrastructure, general Web security issues

2004-01-23 new flaw vulnerability patch fix OpenSSL protocol SSL Sun

NIPC/DHS; http://www.esecurityplanet.com/prodser/article.php/3301661

January 21, eSecurityPlanet — Sun Cluster vulnerable to OpenSSL flaw.

Sun Microsystems on Wednesday, January 21, warned that systems running Sun Cluster 3.x with SunPlex Manager configured were at risk of takeover because of known flaws in the OpenSSL protocol. In a security advisory, Sun recommended that the SunPlex Manager be disabled until a comprehensive patch is ready, warning that exploitation of the vulnerability could lead to arbitrary code execution and denial-of-service (DoS) scenarios. Independent research firm Secunia is rating the vulnerability as "moderately critical." The confirmation of the system access and DoS vulnerabilities comes more than three months after the OpenSSL flaw was made public. Last October, the OpenSSL Project released new versions of its implementation of the Secure Sockets Layer (SSL) and Transport Layer Security (TLS) protocols to plug multiple vulnerabilities. All versions of OpenSSL up to and including 0.9.6j and 0.9.7b and all versions of SSLeay were updated. The OpenSSL project said any application that makes use of OpenSSL's ASN1 library to parse untrusted data was also susceptible. The OpenSSL holes carry a "highly critical" rating. More information can be found at http://sunsolve.sun.com/pub-cgi/retrieve.pl?doc=fsalert/57475

Category 23.6 Web-site infrastructure, general Web security issues

### 2004-02-04 Microsoft Internet Explorer software patch inconsistent user complaint

DHS IAIP Daily; http://news.zdnet.co.uk/internet/security/0,39020375,3914548 7.00.htm

February 04, ZDNet — Users report inconsistent results from latest IE patch.

Microsoft's latest security patch for its Internet Explorer (IE) browser doesn't always work, users report. The fix was supposed to disable a commonly used feature that allows usernames and passwords to be transferred within a URL. However, some users have found that even after the patch is deployed, the "feature" is still active. Microsoft said it has not as yet received any complaints from users experiencing the problems, but tests by ZDNet UK confirm that even after the latest patch is applied, IE still allows URLs containing password and user information to access Internet resources. However, at this stage it is still unclear why some users find the patch works, while others are still left vulnerable.

### 2004-05-18 WS-I SOAP Web services security

DHS IAIP Daily; http://www.esecurityplanet.com/trends/article.php/3355231

May 18, eSecurity Planet — WS- I clears basic security hurdle.

Web services security, a bugbear in the adoption of distributed computing architectures, is one step closer to being finalized. The Web Services Interoperability Organization (WS- I) said it has finished its Basic Security Profile Working Group Draft and is making it available in order to solicit feedback from the Web services community. The Basic Security Profile addresses transport security, SOAP messaging security and other security considerations as well as the interoperability characteristics of two main technologies: HTTP over Transport Layer Security and Web Services Security: SOAP Message Security. Naturally, the Basic Security Profile is expected to synch with other WS- I profiles and work with some existing specifications used to provide security, including the OASIS Web Services Security 1.0 specification, which passed muster last month. When the document is cleaned up and finalized, possibly later this year, it is expected to usher in a raft of new customers to Web services, and by extension service- oriented architectures (SOA).

Category 23.6 Web-site infrastructure, general Web security issues

### 2004-07-29 phpMyAdmin PHP MySQL administration Web development vulnerability

DHS IAIP Daily; http://www.securityfocus.com/bid/10629/info/

July 29, SecurityFocus — phpMyAdmin multiple input validation vulnerabilities.

phpMyAdmin is prone to multiple vulnerabilities. The issues result from insufficient sanitization of user- supplied data. By constructing a URI request for the phpMyAdmin 'left.php' script an attacker may specify and add an arbitrary SQL server. A remote attacker may exploit this vulnerability to replace server configurations and as a result introduce a malicious SQL server into the phpMyAdmin controlled server list. It is also reported that a malicious database table name beginning with "'" will escape the quotes in a PHP eval() statement and will thereby permit an attacker to execute arbitrary PHP code. The vendor has released version 2.5.7, patch level 1 addressing this vulnerability: http://sourceforge.net/index.php

Category 23.6 Web-site infrastructure, general Web security issues

2004-07-30 spam anti-spam pop-up blocker Federal Trade Commission FTC settlement extortion

NewsScan

POP-UP COMPANY AGREES TO PIPE DOWN

D Squared Solutions, a San Diego company founded by two college sudents, has settled with the Federal Trade Commission after agreeing to desist mass-mailing pop-up ads using the Messenger function enabled on many Windows operating systems. D Squared has also agreed to stop peddling

software that would have blocked the very ads it was sending. The company's founders have not admitted any wrongdoing and face no penalties. Their lawyers claimed the pair were not trying to extort consumers with their ads and one attorney suggested that such ads are "annoyances you have to deal with in a free society." (AP 30 July 2004)

Category 23.6 Web-site infrastructure, general Web security issues

2004-08-02 IBM directory server Tivoli vulnerability ldap user exploit fix published

DHS IAIP Daily; http://www.securityfocus.com/bid/10841

August 02, SecurityFocus — IBM Tivoli Directory Server LDACGI Directory Traversal Vulnerability.

IBM Tivoli Directory Server is reported to contain a directory traversal vulnerability in its Web front- end application. This issue presents itself due to insufficient sanitization of user- supplied data. This issue allows remote attackers to view potentially sensitive files on the server that are accessible to the 'ldap' user. This may aid an attacker in conducting further attacks against the vulnerable computer. A fix for Versions 3.2.2 is available here:

http://www-1.ibm.com/support/docview.wss?uid=swg24006917 A fix for Version 4.1 is available here: http://www-1.ibm.com/support/docview.wss?uid=swg24006209

### 2004-08-03 Web server vulnerability note US-CERT BlackJumboDog

DHS IAIP Daily; http://www.kb.cert.org/vuls/id/714584

August 03, US- CERT — Vulnerability Note VU#714584: BlackJumboDog contains a boundary error in the handling of FTP commands.

BlackJumboDog is a multi- function server for Microsoft Windows, providing FTP, Email, Web, and Proxy services. It is reported that version 3.6.1 contains a buffer overflow vulnerability. BlackJumboDog fails to check the length of FTP commands passed to it. Using specially crafted FTP commands, a remote user can trigger a buffer overflow condition possibly leading to code execution on the server. This issue has been resolved in version 3.6.2 of BlackJumboDog: http://homepage2.nifty.com/spw/software/bjd/download.html

Category 23.6 Web-site infrastructure, general Web security issues

### 2004-08-04 portable network graphics PNG library vulnerability open source US-CERT

DHS IAIP Daily; http://www.us- cert.gov/cas/techalerts/TA04- 217A.html

August 04, US- CERT — Technical Cyber Security Alert TA04- 217A: Multiple Vulnerabilities in libpng.

The Portable Network Graphics (PNG) image format is used as an alternative to other image formats such as the Graphics Interchange Format (GIF). The libpng is a popular reference library available for application developers to support the PNG image format. Several vulnerabilities exist in the libpng library, the most serious of which could allow a remote attacker to execute arbitrary code on an affected system. Users should apply the appropriate patch or upgrade as specified by vendor. More detailed information about these vulnerabilities is available in individual vulnerability notes on the US- CERT Website.

### Category 23.6 Web-site infrastructure, general Web security issues

### 2004-08-04 Mozilla Firefox Thunderbird vulnerabilities

DHS IAIP Daily; http://secunia.com/advisories/10856/

August 04, Secunia — Mozilla multiple vulnerabilities.

The vendor has released details about some older vulnerabilities in Mozilla, Mozilla Firefox, and Thunderbird. These can potentially be exploited by malicious people to conduct spoofing attacks, compromise a vulnerable system, or cause a DoS (Denial of Service). The vulnerabilities have reportedly been fixed in: Mozilla 1.7 and higher, Firefox 0.9 and higher, and Thunderbird 0.7 and higher.

Category 23.6 Web-site infrastructure, general Web security issues
--

### 2004-08-04 PHP Bulletin Board phpBB SQL injection vulnerability query patch

DHS IAIP Daily; http://www.securityfocus.com/bid/10868/info/

August 04, SecurityFocus — phpBB Fetch All SQL injection vulnerability .

It is reported that phpBB Fetch All is susceptible to an SQL injection vulnerability. This issue is due to a failure of the application to properly sanitize user- supplied input before using it in an SQL query. The successful exploitation of this vulnerability depends on the implementation of the web application that includes phpBB Fetch All as a component. It may or may not be possible to effectively pass malicious SQL statements to the underlying function. Successful exploitation could result in compromise of the application, disclosure or modification of data or may permit an attacker to exploit vulnerabilities in the underlying database implementation. The vendor has released version 2.0.12 to address this issue: http://prdownloads.sourceforge.net/phpbbfetchall/phpbb\_fetch\_all- 2.0.12.zip?downloa

Category 23.6 Web-site infrastructure, general Web security issues

### 2004-08-04 **PuTTY telnet SSH software vulnerability malicious server connection**

DHS IAIP Daily; http://secunia.com/advisories/12212/

August 04, Secunia — PuTTY unspecified system compromise vulnerability.

A vulnerability in PuTTY can be exploited by malicious people to compromise a user's system. The vulnerability is caused due to an unspecified error and may allow execution of arbitrary code on a user's system. Successful exploitation requires that a user has been tricked into connecting to a malicious server. Users should upgrade to version 0.55.

### 2004-08-05 **Opera Internet browser flaw computer hijack e-mail exposure**

DHS IAIP Daily; http://www.esecurityplanet.com/patches/article.php/3391281

August 05, internetnews.com — Critical flaws spoil Opera tune.

Alternative Web browser firm Opera Software has issued a fix for its Opera browser after a security research firm reported a potentially dangerous security bug. Opera rolled out a new version (7.54) and confirmed that users of previous versions were at risk of computer hijack. GreyMagic, the research outfit that discovered the vulnerabilities, said a successful attack would allow read- access to files on the victim's file system and read access to lists of files and folders on the victim's computer. Malicious hackers could also gain access to read incoming and outgoing e- mails on Opera's M2 mail program, which is built into the browser. The flaws also could result in cookie theft, URL- spoofing for phishing attacks and the spillage of a user's browsing history. GreyMagic also released a proof- of- concept demonstration that presents the user's files and directories in an Explorer- like manner, allowing the user to browse his/her own file system using the vulnerability.

Category 23.6 Web-site infrastructure, general Web security issues

### 2004-08-05 Board Power Internet forum technology vulnerability cross-site scripting attack

### DHS IAIP Daily; http://www.kb.cert.org/vuls/id/744590

August 05, US- CERT — Vulnerability Note VU#744590: Board Power forum contains cross- site scripting vulnerability in the 'action' parameter of 'icq.cgi'.

Board Power is a forum application available for multiple operating systems. It is reported that Board Power v2.04 PF contains a cross- site scripting vulnerability. Board Power fails to filter malicious content passed into the "action" parameter of icq.cgi. Other versions may be affected. It appears that Board Power is no longer supported and has not been updated since 2000 by the developers (The Webmaster Guide, Inc.). The victim will be presented with information which the compromised site did not wish their visitors to be subjected. This could be used to "sniff" sensitive data from within the web page, including passwords, credit card numbers, and any arbitrary information the user inputs. Likewise, information stored in cookies can be stolen or corrupted. US- CERT is currently unaware of a practical solution to this problem.

Category 23.6 Web-site infrastructure, general Web security issues

### 2004-08-10 Apache Webserver vulnerabilities HP VirtualVault HP11 Webproxy patch issued

DHS IAIP Daily; http://secunia.com/advisories/12246

August 10, Secunia — HP VirtualVault / Webproxy multiple vulnerabilities in Apache.

HP has confirmed some vulnerabilities in Apache affecting HP VirtualVault and HP 11 Webproxy, which can be exploited by malicious people to cause a DoS (Denial of Service), bypass security restrictions, or compromise a vulnerable system. The vulnerabilities affect servers running HP- UX release B.11.04 with VirtualVault A.04.50 - A.04.70 or Webproxy A.02.00 - A.02.10 installed. Install patches available at: http://itrc.hp.com

Category 23.6	Web-site infrastructure, general Web security issues
2004-08-10	Microsoft security bulletin Exchange Server vulnerability cross site scripting spoofing

DHS IAIP Daily; http://www.microsoft.com/security/bulletins/200408\_exchange. mspx

August 10, Microsoft — Microsoft Security Bulletin MS04- 026: Vulnerability in Exchange Server 5.5 Outlook Web Access Could Allow Cross- Site Scripting and Spoofing Attacks.

A cross- site scripting and spoofing vulnerability exists in Outlook Web Access for Exchange Server 5.5 that could allow an attacker to convince a user to run a malicious script. An attacker who successfully exploited the vulnerability could manipulate Web browser caches and intermediate proxy server caches, and put spoofed content in those caches. They may also be able to exploit the vulnerability to perform cross- site scripting attacks. Microsoft has assigned a risk rating of "Moderate" to this issue and recommends that customers consider applying the security update. Customers who have customized any of the ASP pages that are listed in the File Information section in this document should back up those files before they apply the update because those ASPs will be overwritten when the update is applied. Any customizations would then have to be reapplied to the new ASP pages.

### 2004-08-13 content management system JetboxOne vulnerability database information disclosure vulnerability US-CERT

DHS IAIP Daily; http://www.kb.cert.org/vuls/id/586720

August 13, US- CERT — Vulnerability Note VU#586720: JetboxOne leaves account database unencrypted.

JetboxOne is an open- source content management system that is written in PHP. An information disclosure vulnerability exists because JetboxOne does not encrypt account information stored in the admin (user) and webuser (standard user) tables of a MySQL database. Any user with the ability to query the database may be able to view confidential account information. This may lead to unauthorized access to other accounts. US- CERT is currently unaware of a practical solution to this problem.

## Category 23.6 Web-site infrastructure, general Web security issues 2004-08-13 content management system JetboxOne vulnerability code execution vulnerability US-CERT

### DHS IAIP Daily; http://www.kb.cert.org/vuls/id/417408

August 13, US- CERT — Vulnerability Note VU#417408: JetboxOne may allow unauthorized users to execute arbitrary code.

JetboxOne, an open- source content management system, could allow an attacker with "AUTHOR" privileges to upload arbitrary files to the image folder via the upload image control. The vulnerability exists because the type of file being uploaded is not verified as a valid image file e.g. GIF, JPEG. Once uploaded, the attacker is then able to request the file, which will be interrpreted by the JetboxOne application. Based on the file type this may permit a malicious user to execute the arbitrary code on the compromised system. Currently, the vulnerability has been demonstrated on version 2.0.8. However, it may also exist in previous versions, but they are as of yet untested. US- CERT is currently unaware of a practical solution to this problem.

### Category 23.6 Web-site infrastructure, general Web security issues

### 2004-08-16 Website services security problems XML code authentication hacking

DHS IAIP Daily;

http://www.computerworld.com/developmenttopics/development/s tory/0,10801,95197,00.html

August 16, Computerworld — Web services security: trouble in transit.

The shareable design of Web services, which gives companies the benefit of easily exchanging data and applications with business partners, also makes them vulnerable to security breaches. Hackers have found ways to tweak the XML code used to tag the data so activity that's actually an attack appears to be valid. According to experts, hackers have three methods for breaching Web services and XML security: identity- based attacks, in which a hacker poses as an authorized user to gain access to Web services; malicious- content attacks, in which an intruder forces a Web server to perform an unauthorized activity; and operational attacks, in which a hacker manipulates an XML message to tie up server resources. But although the methods are known, safeguarding Web services is difficult because multiple elements must be locked down- - the servers, the messages and the applications. Companies must first secure their Web servers and then decide which business partners and employees will have access to them, how they'll connect to them and which authentication method to use.

Category 23.6 Web-site infrastructure, general Web security issues

### 2004-08-20 Mozilla buffer overflow vulnerability POP3 protocol

DHS IAIP Daily; http://www.kb.cert.org/vuls/id/561022

August 20, US- CERT — Vulnerability Note VU#561022: Mozilla contains a buffer overflow in the SendUidl() function.

Post Office Protocol Version 3 (POP3) is a mail protocol that provides a means for retrieving email from a remote server. This protocol is supported by Mozilla, Firefox, and Thunderbird. These clients contain a vulnerability that allows malformed POP3 responses to trigger a buffer overflow condition in the SendUidl() function. Such responses can be sent by a remote POP3 server and could result in arbitrary code execution. Exploitation of this vulnerability would require a user to connect to a malicious POP3 server. This issue has been resolved in Mozilla 1.7, Firefox 0.9, and Thunderbird 0.7.2: http://www.mozilla.org/projects/security/known- vulnerabiliti es.html

### 2004-08-20 MySQL buffer overflow vulnerability DNS lookup

DHS IAIP Daily; http://www.zone- h.org/advisories/read/id=5365

August 20, zone- h — MySQL "mysql\_real\_connect" buffer overflow vulnerability.

A vulnerability in MySQL could potentially allow malicious people to compromise a vulnerable system. The "mysql\_real\_connect()" function doesn't properly verify the length of IP addresses returned by a reverse DNS lookup of a hostname. This could potentially be exploited to cause a buffer overflow and execute arbitrary code. Successful exploitation requires that the attacker is able to return a malicious DNS reply when a MySQL user connects to a server. This has been reported in MySQL 4.0.20 and prior. It has been reported that this can't be exploited on the Linux and OpenBSD platforms. This issue will be fixed in the upcoming 4.0.21. Original Advisory: http://bugs.mysql.com/bug.php?id=4017

### Category 23.6 Web-site infrastructure, general Web security issues

### 2004-08-23 Mozilla Firefox Thunderbird vulnerability X.509 certificate verification failure

DHS IAIP Daily; http://www.kb.cert.org/vuls/id/784278

August 23, US- CERT — Vulnerability Note VU#784278: Mozilla allows certificate to be imported even when the DN is the same as that of a built- in CA root certificate.

Mozilla version 1.7.7 fails to verify that the Distinguished Name (DN) of an X.509 certificate is unique when importing it. A denial of service occurs when Mozilla imports a specially crafted self- signed certificate that has the same DN as an existing Certificate Authority (CA) root certificate. Exploitation of this vulnerability can be automated causing the certificate to be imported without any user intervention. A remote attacker could cause a denial of service against the certificate store, preventing the user from accessing SSL websites. This issue has been resolved in Mozilla 1.7.2, Firefox 0.9.3, and Thunderbird 0.7.3: http://www.mozilla.org/projects/security/known- vulnerabilities.html

# Category 23.6 Web-site infrastructure, general Web security issues 2004-08-23 buffer overflow Netscape Network Security Services NSS suite Secure Sockets Layer SSL

DHS IAIP Daily; http://xforce.iss.net/xforce/alerts/id/180

August 23, Internet Security Systems — Netscape NSS Library remote compromise.

A vulnerability exists in the Netscape Network Security Services (NSS) library suite which may result in remote compromise of products making use of this library for Secure Sockets Layer (SSL) communication. If the SSLv2 protocol is enabled on vulnerable servers, a remote unauthenticated attacker may trigger a buffer overflow condition and execute arbitrary code. This has the potential to result in complete compromise of the target server, and exposure of any information held therein. SSL is often used to secure sensitive or valuable communications, making this a high- value target for attackers. A vendor- supplied update for the NSS library is available: ftp.mozilla.org/pub/mozilla.org/security/nss/releases/NSS\_3\_9\_2\_RTM

Category 23.6 Web-site infrastructure, general Web security issues

### 2004-08-24 Sun Solaris Apache vulnerabilities denial of service DoS code execution attack

DHS IAIP Daily; http://sunsolve.sun.com/pub- cgi/retrieve.pl?doc=fsalert/5762 8

August 24, Sun Microsystems — Sun Solaris multiple Apache vulnerabilities.

Multiple vulnerabilities exist in Apache for Solaris, which can be exploited to bypass certain security restrictions, cause a DoS (Denial of Service), or potentially compromise a vulnerable system. The Apache HTTP process normally runs as the unprivileged uid "nobody." The ability to execute arbitrary code as the unprivileged uid "nobody" may lead to modified web content, denial of service, or further compromise. While a final vendor solution is pending, patches are available at: http://sunsolve.sun.com/tpatches

Category 23.6 Web-site infrastructure, general Web security issues

### 2004-09-02 Opera 7.23 Internet Web browser embed tag HTML crash vulnerability

DHS IAIP Daily; http://www.securitytracker.com/alerts/2004/Sep/1011142.html

September 02, SecurityTracker — Opera 'embed' tag error lets remote users crash the browser.

A vulnerability exists in the Opera browser 7.23 build 3227 in the processing of the 'embed' tag. A remote user can create HTML that, when loaded by the target user, will cause the target user's browser to crash. Update to version 7.51: http://www.opera.com/

### IYIR 2004

Category 23.6 Web-site infrastructure, general Web security issues

### 2004-09-02 secure shell OpenSSH SSH default configuration unsafe CVS

DHS IAIP Daily; http://www.securitytracker.com/alerts/2004/Sep/1011143.html

September 02, SecurityTracker — OpenSSH default configuration may be unsafe when used with anonymous SSH services.

A configuration vulnerability exists in the default configuration of OpenSSH 3.9 and prior when used with anonymous public services such as anonymous CVS. A remote user can connect to arbitrary hosts via the target service. Affected sites can place the following statement in their '/etc/ssh/sshd\_config' configuration file to prevent attacks: AllowTcpForwarding no

Category 23.6	Web-site infrastructure, general Web security issues
2004-09-03	Juniper Network NetScreen IDP SSH server file overwrite vulnerability secure copy
	scp

DHS IAIP Daily; http://www.securitytracker.com/alerts/2004/Sep/1011144.html

September 03, SecurityTracker — Juniper Networks NetScreen- IDP may let remote SSH Servers overwrite files in certain cases.

A vulnerability exists in Juniper Networks NetScreen IDP that could allow a remote SSH server to overwrite arbitrary files on the target system in certain situations. This is due to an underlying directory traversal vulnerability in scp, the report said. This could lead to a remote SSH server being able to overwrite arbitrary files on the target system in certain situations. Original advisory and resolutions: http://www.juniper.net/support/security/alerts/adv59739.txt

Category 23.6 Web-site infrastructure, general Web security issues

### 2004-09-15 Internet Web browser session fixation attack vulnerability no solution

DHS IAIP Daily; http://www.westpoint.ltd.uk/advisories/wp-04-0001.txt

September 15, Westpoint Security Advisory — Several Internet browsers have session fixation vulnerability.

A vulnerability was reported in Microsoft Internet Explorer, KDE Konqueror, Mozilla Firefox, and Opera that may allow a remote user to set cookies on via a non- secure server to be sent to a secure server as part of a Session Fixation Attack. This flaw may allow remote users to hijack a target user's session. No solution is currently available; refer to Westpoint Security Advisory for workarounds.

Category 23.6 Web-site infrastructure, general Web security issues

2004-09-20 Sun Java NSS library heap buffer overflow SSLv2 vulnerability update issued

DHS IAIP Daily; http://secunia.com/advisories/12599

September 20, Secunia — Sun Java Enterprise System NSS library vulnerability.

Sun has acknowledged a vulnerability in the NSS library included with Sun Java Enterprise System. This vulnerability was originally reported on August 25 and is caused due to a boundary error within the parsing of records during SSLv2 connection negotiation. The vulnerability can be exploited to cause a heap- based buffer overflow by sending a specially crafted client hello message with an overly long record. Successful exploitation allows execution of arbitrary code with the privileges of an application linked to the vulnerable library. Original advisory and workaround: http://sunsolve.sun.com/search/document.do?assetkey=1- 26- 576 43- 1

Category 23.6 Web-site infrastructure, general Web security issues

### 2004-09-30 **OpenSSL temporary file creation vulnerability update issued**

DHS IAIP Daily; http://www.securityfocus.com/bid/11293

September 30, SecurityFocus — OpenSSL unspecified insecure temporary file creation vulnerability.

OpenSSL is affected by an unspecified insecure temporary file creation vulnerability. This issue is likely due to a design error that causes the application to fail to verify the existance of a file before writing to it. Updates available at: ftp://ftp.trustix.org/pub/trustix/updates/

# Category 23.6 Web-site infrastructure, general Web security issues 2004-10-19 Microsoft Internet Explorer vulnerabilities code execution privilege escalation update Windows XP SP2

DHS IAIP Daily; http://www.us- cert.gov/cas/techalerts/TA04- 293A.html

October 19, US- CERT — Technical Cyber Security Alert TA04- 293A: Multiple Vulnerabilities in Microsoft Internet Explorer.

Microsoft Internet Explorer (IE) contains multiple vulnerabilities, the most severe of which could allow a remote attacker to execute arbitrary code with the privileges of the user running IE. Microsoft Security Bulletin MS04- 038 describes a number of IE vulnerabilities, including buffer overflows, cross- domain scripting, spoofing, and "drag and drop." The impacts of these vulnerabilities vary, but an attacker may be able to execute arbitrary code with the privileges of the user running IE. Solutions: Apply the appropriate patch as specified by Microsoft Security Bulletin MS04- 038; disable Active scripting and ActiveX controls; upgrade to Windows XP Service Pack 2. Microsoft Security Bulletin MS04- 038: http://www.microsoft.com/technet/security/bulletin/ms04- 038.mspx

Category 23.6 Web-site infrastructure, general Web security issues

### 2004-10-27 website blocking Bush foreign access controls

NewsScan; http://www.washingtonpost.com/wp-dyn/articles/A2668-2004Oct27.html

BUSH WEB SITE BLOCKS FOREIGN VISITORS

The Bush-Cheney campaign has cut off access to its Web site by anyone outside the U.S. or Canada. Instead, those visitors will see the message: "Access denied. You don't have permission to access www.georgewbush.com on this server." The move comes a week after a crippling hacker attack that took down the Web site for six hours. Security experts say that while it's not usual for Web sites to block traffic from specific Internet addresses or from certain countries notorious for churning out spam, the Bush-Cheney campaign's move is probably unprecedented. "I've never heard of a site wholesale blocking access from the rest of the world," says Johannes Ulrich, CTO for the SANS Internet Storm Center. "I guess they decided it just wasn't worth the trouble to leave it open to foreign visitors." Jonah Sieger, a founding partner for Connections Media, which does consulting work with Democratic candidates, says it doesn't make sense for the Bush-Cheney folks to "consciously block access to anybody. Maybe the next thing they'll try is to block Democrats and people in blue states from coming to the site." (Washington Post 27 Oct 2004)

Category 23.6 Web-site infrastructure, general Web security issues	
--	--

### 2004-11-01 browsers Internet Explorer Firefox Safari Mozilla Opera study

NewsScan; http://news.com.com/Study+Firefox+still+gaining+on+Internet+Explorer/2100-1032\_3-5435176.html

IE LOSING GROUND TO OPEN SOURCE BROWSERS

Microsoft's Internet Explorer browser is still the overwhelming market leader, but the percentage of Americans using opensource alternatives Mozilla and Firefox inched up to 6% in October from 3.5% in June. Apple's Safari and the Opera browsers combined were employed by just a little over 1% of users, according to online research firm WebSideStory. The results were gleaned by sensors embedded on major Web sites that identified which browsers visitors were using to access the sites. And although Mozilla and Firefox constitute a miniscule portion of the browser market, some analysts say their steady rise may signal a trend. "What we're seeing is (Mozilla and Firefox) looking more like a vanguard than a flash in the pan," says WebSideStory analyst Geoff Johnston. (CNet News.com 1 Nov 2004)

Category 23.6 Web-site infrastructure, general Web security issues

### 2004-11-04 Apache Web server software Space Headers denial of service DoS vulnerability update issued

DHS IAIP Daily; http://secunia.com/advisories/13045/

November 04, Secunia — Apache "Space Headers" denial of service vulnerability.

A vulnerability has been discovered in Apache, which can be exploited by malicious people to cause a DoS (Denial of Service). The vulnerability is caused due to an error in the parsing routine for headers with a large amount of spaces. This can be exploited by sending some specially crafted requests with a large amount of overly long headers containing only spaces. The vulnerability has been fixed in version 2.0.53- dev.

### 2004-11-09 Microsoft Internet Explorer URL Handler vulnerability Windows XP SP2 update

DHS IAIP Daily; http://secunia.com/advisories/13124/

November 09, Secunia — Microsoft Internet Explorer "res:" URI Handler file identification vulnerability. A vulnerability has been discovered in Internet Explorer, which can be exploited by malicious sites to detect the presence of local files. An "Access is Denied" error will be returned if a site in the "Internet" zone tries to open an existing local file in the search window using the "res:" URI handler. This can be exploited to determine the presence of specific programs or files in the system directories and on the desktop. The vulnerability has been confirmed on a fully patched system with Internet Explorer 6.0 and Microsoft Windows XP SP1. The vulnerability does not affect systems running Windows XP with SP2 installed.

Category 23.6	Web-site infrastructure, general Web security issues
2004-11-10	spoofing vulnerability Microsoft Internet Security and Acceleration ISA server 200 Proxy 2.0 update issued

DHS IAIP Daily;

http://www.microsoft.com/technet/security/bulletin/ms04-039.mspx

November 10, Microsoft — Spoofing vulnerability in Microsoft Servers.

A spoofing vulnerablity exists in Microsoft Internet Security and Acceleration (ISA) Server 2000 and Microsoft Proxy Server 2.0 that could enable an attacker to spoof trusted Internet content. Users could believe they are accessing trusted Internet content when in reality they are accessing malicious Internet content, for example a malicious Website. Microsoft rates this vulnerability as Important and recommends users install updates described in Microsoft Security Bulletin MS04- 039 available through the Source link below.

# Category 23.6 Web-site infrastructure, general Web security issues 2004-11-10 Microsoft Internet Explorer IE buffer overflow vulnerability code execution attack Windows XP SP2 update

DHS IAIP Daily; http://www.uscert.gov/cas/techalerts/TA04- 315A.html

November 10, US- CERT — Technical Cyber Security Alert TA04- 315A: Buffer Overflow in Microsoft Internet Explorer.

Microsoft Internet Explorer (IE) 6.0 and later contain a buffer overflow vulnerability that could allow a remote attacker to execute arbitrary code with the privileges of the user running IE. A buffer overflow vulnerability exists in the way IE handles the SRC and NAME attributes of various elements, including FRAME, IFRAME, and EMBED. Because IE fails to properly check the size of the NAME and SRC attributes, a specially crafted HTML document can cause a buffer overflow in heap memory. Reports indicate that this vulnerability is being exploited by malicious code propagated via e- mail. IE opens and displays an HTML document that exploits the vulnerability. This malicious code may be referred to as MyDoom or Bofra. Until a complete solution is available from Microsoft, consider the following workarounds: install Windows XP SP2 (SP2 does not appear to be affected by this vulnerability), disable Active scripting, do not follow unsolicited links, read and send e- mail in plain text format, and maintain updated anti- virus software.

Category 23.6 Web-site infrastructure, general Web security issues

2004-11-11 phone companies cybersecurity AT&T Sprint network security programs filtering viruses

NewsScan; http://online.wsj.com/article/0

PHONE COMPANIES TACKLE CYBERSECURITY

As owners of some of the worlds biggest Internet conduits, telephone companies like AT&T and Sprint are in a prime position to monitor Internet activity and stop mischief makers long before they reach the desktops of corporate customers. AT&T recently launched a network security system called Internet Protect and Sprint offers a similar service called IP Defender. Meanwhile, Internet security firm McAfee is marketing a "Clean Pipes" service designed to help carriers purge attacks as they traverse carrier networks. Other big players in the cybersecurity realm include IBM, Symantec and VeriSign, and equipment makers like Cisco and Juniper Networks are embedding security features into their data-routing gear as well. A recent study by Symantec shows a fourfold increase in the number of new viruses attacking Windows computers, to 4,496 in the first half of 2004 -- the largest increase the company has ever documented. Based on numbers like that, Yankee Group predicts that the managed security services market will expand from \$1.5 billion in 2002 to \$3.7 billion in 2008. (Wall Street Journal 11 Nov 2004)

### 2004-11-14 Microsoft Internet Explorer Windows XP SP2 vulnerability code execution attack no update issued

DHS IAIP Daily; http://www.securitytracker.com/alerts/2004/Nov/1012234.html

November 14, SecurityTracker — Microsoft Internet Explorer on XP SP2 remote user vulnerability.

A remote user can bypass the file download security mechanism in Windows XP SP2 and can execute arbitrary scripting code in the local computer zone to take full control of the target user's system. No solution is currently available.

Category 23.6 Web-site infrastruct	ture, general Web security issues
------------------------------------	-----------------------------------

### 2004-11-18 Microsoft Internet Explorer vulnerabilities Windows XP SP2 no update

DHS IAIP Daily; http://secunia.com/advisories/13203/

November 18, Secunia — Microsoft Internet Explorer vulnerabilities.

Two vulnerabilities have been reported in Internet Explorer, which can be exploited by malicious people to bypass a security feature in Microsoft Windows XP SP2 and trick users into downloading malicious files. 1) Microsoft Windows XP SP2 has a security feature which warns users when opening downloaded files of certain types. The problem is that if the downloaded file was sent with a specially crafted "Content- Location" HTTP header in some situations, then no security warning will be given to the user when the file is opened. 2) An error when saving some documents using the Javascript function "execCommand()", can be exploited to spoof the file extension in the "Save HTML Document" dialog. There is no solution at this time.

## Category 23.6 Web-site infrastructure, general Web security issues 2004-11-20 Microsoft Internet Explorer IE unauthorized download vulnerability no update issued

DHS IAIP Daily; http://www.securitytracker.com/alerts/2004/Nov/1012288.html

November 20, SecurityTracker — Microsoft IE Custom 404 error message and execCommand SaveAs permit unauthorized downloads.

A remote user can create HTML that, when loaded by the target user, will prompt the user to download a file but will bypass the XP SP2 executable download warning messages. A remote user can invoke the execCommand 'SaveAs' function via a custom HTTP 404 Not Found error message to download arbitrary files to the target user's system without the XP SP2 warning messages. It is reported that Internet Explorer (IE) does not properly process URLs with certain extraneous characters. A remote user can create a custom HTTP 404 error message and pass this message to the execCommand Method to bypass the 'File Download' and 'File Open' security warnings. There is no solution at this time.

Category 23.6 Web-site infrastructure, general Web security issues

### 2004-11-22 Sun Java JavaScript plugin vulnerability Virtual Machine code execution attack

DHS IAIP Daily; http://www.idefense.com/application/poi/display?id=158

November 22, iDEFENSE — Sun Java Plug- in Java- to- Javascript bug lets remote applets execute arbitrary code.

Remote exploitation of a design vulnerability in Sun Microsystems Inc.'s Java Plug- in technology allows attackers to bypass the Java sandbox and all security restrictions imposed within Java Applets. The problem specifically exists within the access controls of the Java to Javascript data exchange in Web browsers using Sun's Java Plug- in technology. The vulnerability allows Javascript code to load an unsafe class which should not normally be possible from a Java Applet. Successful exploitation allows remote attackers to execute hostile Applets that can access, download, upload or execute arbitrary files as well as access the network. A target user must be running a browser on top of a vulnerable Java Virtual Machine to be affected. The vendor has issued a fixed version (1.4.2\_06), available at: http://java.sun.com/j2se/1.4.2/download.html

Category 23.6 Web-site infrastructure, general Web security issues

### 2004-11-29 WS FTP file transfer protocol server buffer overflow vulnerability code execution attack no update issued

DHS IAIP Daily; http://www.securitytracker.com/alerts/2004/Nov/1012353.html

November 29, SecurityTracker — WS\_FTP buffer overflow lets remote users execute arbitrary code. A remote user can execute arbitrary code on the target system. It is reported that a remote authenticated user can trigger a buffer overflow in several FTP commands. The SITE, XMKD, MKD, and RFNR FTP commands are affected. A remote user can cause the FTP service to crash or execute arbitrary code. No solution is available at this time.

### 2004-11-29 vulnerabilities Mozilla Firefox Safari Opera browsers patches

NewsScan; http://www.internetnews.com/security/article.php/3440971

NEW BROWSER VULNERABILITY TARGETS NON-IE MODELS, TOO

Since its debut, Microsoft's Internet Explorer browser has been plagued by a steady stream of "flaw discovery" announcements followed by the requisite patches. Usually those flaws are exclusive to the Microsoft model, but a new vulnerability also affects the Mozilla Browser, Mozilla Firefox, Opera and Apple Safari browsers. This latest bug, called the Infinite Array Sort Denial of Service Vulnerability, causes the affected browsers to execute an infinite JavaScript array sort, which in turn causes a crash. The flaw was discovered by independent security researcher Berend-Jan Wever, who also uncovered the IFRAME vulnerability that affects banner ads. (InternetNews 29 Nov 2004)

# Category23.6Web-site infrastructure, general Web security issues2004-11-30CuteFTP file transfer protocol server denial of service DoS vulnerability code<br/>execution attack no update issued

DHS IAIP Daily; http://www.securitytracker.com/alerts/2004/Nov/1012366.html

November 30, SecurityTracker — CuteFTP Professional FTP reply error remote denial of service.

A remote FTP server can cause the target connected FTP client to crash. It is reported that a connected FTP server can send a specially crafted reply code (generally larger than "500") and specially crafted text larger than 65530 bytes to cause the client to crash. Only replies to certain commands are affected. This flaw could possibly be exploited to execute arbitrary code. No solution is available at this time.

# Category 23.6 Web-site infrastructure, general Web security issues 2004-12-01 Microsoft security bulletin update Internet Explorer IE vulnerability code execution privilege escalation attack

DHS IAIP Daily;

http://www.microsoft.com/technet/security/bulletin/MS04- 040. mspx

December 01, Microsoft — Microsoft Security Bulletin MS04- 040: Cumulative Security Update for Internet Explorer.

A vulnerability exists in Internet Explorer that could allow remote code execution on an affected system. An attacker could exploit the vulnerability by constructing a malicious Web page that could potentially allow remote code execution if a user visited a malicious Website. If a user is logged on with administrative privileges, an attacker who successfully exploited this vulnerability could take complete control of an affected system. Microsoft has assigned a risk rating of "Critical" to this issue and recommends that customers install the update immediately.

Category 23.6 Web-site infrastructure, general Web security issues

2004-12-02 Cisco CNS Network Registrar DNS DHCP server denial of service DoS vulnerability update issued

DHS IAIP Daily;

http://www.cisco.com/warp/public/707/cisco- sa- 20041202- cnr.s html

December 02, Cisco Security Advisory — Cisco CNS Network Registrar denial of service vulnerability.

Cisco CNS Network Registrar Domain Name Service /Dynamic Host Configuration Protocol (DNS/DHCP) server for the Windows Server platforms is vulnerable to a Denial of Service attack when a certain crafted packet sequence is directed to the server. Cisco CNS Network Registrar version 6.0 through 6.1.1.3 are affected by CSCeg27625. However, all versions up to and including version 6.1.1.3 are also affected by CSCeg27614. Cisco has made free software available to address this vulnerability for all affected customers.

2004-12-03 Apple Darwin Streaming Server null byte denial of service DoS attack update issued

DHS IAIP Daily;

http://www.idefense.com/application/poi/display?id=159&type= vulnerabilities&flashstatus=true

December 03, iDEFENSE — Apple Darwin Streaming Server DESCRIBE null byte denial of service vulnerability.

Remote exploitation of an input validation vulnerability in Apple Computer Inc.'s Darwin Streaming Server allows attackers to cause a denial of service condition. The vulnerability specifically occurs due to insufficient sanity checking on arguments to DESCRIBE requests. A remote attacker can send a request for a location containing a null byte to cause a denial of service condition, thereby preventing legitimate users from accessing streamed content. Updates are available at: http://www.apple.com/support/downloads//

Category 23.6 Web-site infrastructure, general Web security issues

2004-12-07 Unicenter Remote Control access management server vulnerability update issued

DHS IAIP Daily; http://secunia.com/advisories/13311/

December 07, Secunia — Unicenter Remote Control arbitrary URC Management Server access vulnerability.

A vulnerability has been reported in Unicenter Remote Control (URC), which can be exploited by malicious users to access arbitrary URC Management Servers. The vulnerability is caused due to an unspecified error in the URC Management Console allowing users to connect to another URC Management Server and make arbitrary configuration changes on the systems managed by this server. Successful exploitation reportedly requires that a user has been authenticated by the underlying OS. Updates available at: http://supportconnectw.ca.com/public/rco\_controlit/infodocs/ securitynotice.asp

Category 23.6	Web-site infrastructure, general Web security issues
2004-12-09	Microsoft Internet Explorer IE 6.0 file transfer protocol FTP command injection vulnerability Windows 2000 2K SP4 XP SP2 no update issued

DHS IAIP Daily; http://secunia.com/advisories/13404/

December 09, Secunia — Microsoft Internet Explorer FTP command injection vulnerability.

A vulnerability has been reported in Microsoft Internet Explorer, which can be exploited by malicious people to conduct FTP command injection attacks. The vulnerability is caused due to insufficient input validation of FTP URIs. This can be exploited by e.g. a malicious website to inject arbitrary FTP commands in a FTP session using a specially crafted pathname containing "%0A" characters. The vulnerability has been confirmed on a fully patched system with Internet Explorer 6.0 and Microsoft Windows 2000 SP4 / XP SP2. There is no solution at this time.

Category 23.6 Web-site infrastructure, general Web security issues

### 2004-12-10 MIMEsweeper SMTP PDF denial of service DoS vulnerability

DHS IAIP Daily; http://secunia.com/advisories/13411/

December 10, Secunia — MIMEsweeper for SMTP PDF file processing denial of service.

A vulnerability has been reported in MIMEsweeper for SMTP, which can be exploited by malicious people to cause a DoS (Denial of Service). The vulnerability is caused due to an error within the Security Service when processing PDF files. This can be exploited to crash the Security Service by sending an e- mail containing a specially crafted PDF file as attachment. Apply MIMEsweeper for SMTP 5.0 Service Pack 1: http://www.clearswift.com/download/info.aspx?ID=562

2004-12-13 phpBB PHP bulletin board Web software vulnerabilities directory traversal attack update issued

DHS IAIP Daily; http://secunia.com/advisories/13421/

December 13, Secunia — phpBB Attachment Mod two vulnerabilities.

Two vulnerabilities have been reported in the Attachment Mod module for phpBB, which can be exploited by malicious people to compromise a vulnerable system. An input validation error can be exploited to add, remove, and execute files outside the upload directory via directory traversal attacks. Secondly, an error in the handling of multiple file extensions within "mod\_mime" can be exploited to upload malicious script files. The vulnerabilities have been reported in version 2.3.10. Update to version 2.3.11: http://sourceforge.net/project/showfiles.php?group\_id=66311

Category 23.6 Web-site infrastructure, general Web security issues

#### 2004-12-14 phpMyAdmin PHP MySQL Web scripting software update issued

DHS IAIP Daily; http://secunia.com/advisories/13424/

December 14, Secunia — phpMyAdmin two vulnerabilities.

Two vulnerabilities exist in phpMyAdmin, which can be exploited by malicious people to compromise a vulnerable system and by malicious users to disclose sensitive information. An input validation error in the handling of MySQL data allows injection of arbitrary shell commands. Input passed to "sql\_localfile" is not properly sanitized in "read\_dump.php" before being used to disclose files. Successful exploitation requires access to the phpMyAdmin interface, and that PHP safe mode is disabled and the UploadDir mechanism to be active. The vulnerabilities have been fixed in version 2.6.1- rc1.

#### Category 23.6 Web-site infrastructure, general Web security issues 2004-12-14 zgv xzgv integer overflow vulnerabilities compromise code execution attack update issued

DHS IAIP Daily; http://secunia.com/advisories/13449/

December 14, Secunia — zgv/xzgv multiple integer overflow vulnerabilities.

Multiple vulnerabilities have been reported in zgv/xzgv, which potentially can be exploited by malicious people to compromise a vulnerable system. The vulnerabilities are caused due to various integer overflows when processing images. These can be exploited to cause buffer overflows via images containing specially crafted headers. Successful exploitation may allow execution of arbitrary code when a malicious image is viewed. Apply patches: http://rus.members.beeb.net/xzgv- 0.8- integer- overflow- fix.di ff

Category 23.6 Web-site infrastructure, general Web security issues

2004-12-16 Cisco Unity default usernames passwords Exchange vulnerability update issued

DHS IAIP Daily; http://secunia.com/advisories/13483/

December 16, Secunia — Cisco Unity default usernames and passwords vulnerability.

A security issue has been reported in Cisco Unity versions 2.x, 3.x, and 4.x (prior to version "4.0(5)") when integrated with Exchange, which can be exploited by malicious people to access administrative functions. The problem is that Cisco Unity creates certain user accounts with default passwords when integrated with Exchange. Successful exploitation provides access to certain administrative functions. A vendor solution is available at:

http://www.cisco.com/warp/public/707/cisco- sa- 20041215- unity .shtml

Category 23.6 Web-site infrastructure, general Web security issues

#### 2004-12-16 PHP Web scripting language multiple vulnerabilities update issued

DHS IAIP Daily; http://secunia.com/advisories/13481/

December 16, Secunia — PHP multiple vulnerabilities.

Multiple vulnerabilities have been reported in PHP, which can be exploited to gain escalated privileges, bypass certain security restrictions, gain knowledge of sensitive information, or compromise a vulnerable system. Update to version 4.3.10 or 5.0.3: http://www.php.net/downloads.php

2004-12-16 Samba security integer overflow heap based buffer overflow vulnerability update issued

DHS IAIP Daily; http://secunia.com/advisories/13453

December 16, Secunia — Samba security descriptor parsing integer overflow vulnerability.

A vulnerability has been reported in Samba versions 2.x and 3.0.x up to and including version 3.0.9, which can be exploited by malicious users to compromise a vulnerable system. The vulnerability is caused due to an integer overflow within smbd when handling security descriptors. This can be exploited to cause a heap- based buffer overflow by requesting an extremely large amount of security descriptors. Successful exploitation allows execution of arbitrary code, but requires that the user has proper credentials to access a share. Apply patch for Samba 3.0.9: http://us1.samba.org/samba/ftp/patches/security/samba- 3.0.9- CAN- 2004- 1154.patch

Category 2	23.6	Web-site infrastructure.	general Web security issues
------------	------	--------------------------	-----------------------------

### 2004-12-17 Symantec Brightmail software vulnerabilities denial of service DoS update issued

DHS IAIP Daily; http://secunia.com/advisories/13489/

December 17, Secunia — Symantec Brightmail denial of service vulnerabilities.

Two vulnerabilities have been reported in Symantec Brightmail, which can be exploited by malicious people to cause a DoS (Denial of Service). The Sieve module fails to recognize malformed RFC 822 MIME attachment boundaries and Spamhunter fails to convert certain valid character encoding sets to UTF. Apply patch 134: ftp://ftp.symantec.com/public/english\_us\_canada/products/sba/sba\_60x/updates/Patch134.zip

# Category 23.6 Web-site infrastructure, general Web security issues 2004-12-21 US CERT phpBB PHP bulletin board highlight parameter vulnerability Website hacking update issued

DHS IAIP Daily; http://www.us- cert.gov/cas/techalerts/TA04- 356A.html

December 21, US- CERT — Technical Cyber Security Alert TA04- 356A: Exploitation of phpBB highlight parameter vulnerability.

The software phpBB, an open- source bulletin board application, contains an input validation problem in how it processes a parameter contained in URLs. An intruder can deface a phpBB Website, execute arbitrary commands, or gain administrative privileges on a compromised bulletin board. According to reports, this vulnerability is being actively exploited by the Santy.A worm. The worm appears to propagate by searching for the keyword "viewtopic.php" in order to find vulnerable sites. The worm writes itself to a file named "m1ho2of" and then overwrites files ending with .htm, .php, .asp. shtm, .jsp, and .phtm replacing them with HTML content that defaces the Web page. Upgrade to phpBB version 2.0.11: http://www.phpbb.com/downloads.php

Category 23.6 Web-site infrastructure, general Web security issues

2004-12-30 Mozilla Internet Web browser buffer overflow vulnerability code execution attack update issued

DHS IAIP Daily; http://securitytracker.com/alerts/2004/Dec/1012726.html

December 30, SecurityTracker — Mozilla buffer overflow in processing NNTP URLs lets remote users execute arbitrary code.

A heap overflow vulnerability was reported in Mozilla in the processing of NNTP URLs. A remote user can create a specially crafted 'news://' URL that, when loaded by the target user, will trigger a buffer overflow and execute arbitrary code on the target user's system. The code will run with the privileges of the target user. The vendor has issued a fixed version (1.7.5), available at: http://www.mozilla.org/products/mozilla1.x/

## 23.7 VoIP

Category 23.7	VoIP
2004-01-14	VoIP voice over IP flaw weakness hole exploit text messaging Microsoft Cisco crash denial of service DoS

RISKS; http://news.com.com/2100-1002\_3-5140284.html?tag=nefd\_lede 23

FLAWS THREATEN VOIP NETWORKS

Peter G. Neumann produced this abstract of an article by Robert Lemos in CNET News:

A technical review conducted by the British government has found several security flaws in products that use VoIP and text messaging, including those from Microsoft and Cisco Systems. The flaws affect software and hardware that support the real-time multimedia communications and processing standard, known as the International Telecommunications Union (ITU) H.323 standard.

The security problems can cause a product that supports H.323 to crash. For example, in Cisco telecommunications products running its IOS operating system, the vulnerability could be used to cause the devices to freeze or reboot. However, on Microsoft's Internet Security and Acceleration Server 2000, which is included with Small Business Server 2000 and 2003 editions, the vulnerability could allow an attacker to take control of the system.

Category 23.7 VoIP

### 2004-01-15 **CERT CC advisorty message vulnerability flaw patch fix**

NIPC/DHS; http://www.cert.org/advisories/CA- 2004- 01.html

January 13, CERT/CC, NISCC — CERT Advisory CA-2004-01 Multiple H.323 Message Vulnerabilities.

The U.K. National Infrastructure Security Co-ordination Centre has reported multiple vulnerabilities in different vendor implementations of the multimedia telephony protocol H.323. H.323 is an international standard protocol, published by the International Telecommunications Union, used to facilitate communication among telephony and multimedia systems. Examples of such systems include VoIP, video-conferencing equipment, and network devices that manage H.323 traffic. Exploitation of these vulnerabilities may result in the execution of arbitrary code or cause a denial of service, which in some cases may require a system reboot. Systems administrators should apply a patch or upgrade and filter network traffic. Sites should apply network packet filters to block access to the H.323 services at network borders, including 1720/TCP and 1720/UDP. If access cannot be filtered at the network perimeter, the CERT/CC recommends limiting access to only those external hosts that require H.323 for normal operation. Some firewalls process H.323 packets and may themselves be vulnerable to attack. Certain sites may actually want to disable application layer inspection of H.323 network packets. Additional information is available on the Microsoft Website:

http://www.microsoft.com/technet/treeview/default.asp?url=/t echnet/security/bulletin/ms04-001.asp

# Category 23.7 VoIP 2004-01-15 CERT/CC advisory message vulnerability flaw patch fix VoIP multimedia messaging telephony protocols TCP UDP

### DHS/IAIP Update

CERT ADVISORY CA- 2004- 01 MULTIPLE H.323 MESSAGE VULNERABILITIES.

The U.K. National Infrastructure Security Coordination Centre has reported multiple vulnerabilities in different vendor implementations of the multimedia telephony protocol H.323. H.323 is an international standard protocol, published by the International Telecommunications Union, used to facilitate communication among telephony and multimedia systems. Examples of such systems include VoIP, video- conferencing equipment, and network devices that manage H.323 traffic. Exploitation of these vulnerabilities may result in the execution of arbitrary code or cause a denial of service, which in some cases may require a system reboot. Systems administrators should apply a patch or upgrade and filter network traffic. Sites should apply network packet filters to block access to the H.323 services at network borders, including 1720/TCP and 1720/UDP. If access cannot be filtered at the network perimeter, the CERT/CC® recommends limiting access to only those external hosts that require H.323 for normal operation. Some firewalls process H.323 packets and may themselves be vulnerable to attack. Certain sites may actually want to disable application layer inspection of H.323 network packets. Additional information is available on the Microsoft Website:

 $http://www.microsoft.com/technet/treeview/default.asp?url=/t\ echnet/security/bulletin/ms04-\ 001.asp$ 

21

Category 23.7 VoIP

2004-01-23 Cisco voice product security flaw vulnerability patch fix

NIPC/DHS; http://www.cisco.com/warp/public/707/cisco-sa-20040121-voice.shtml

January 22, earthweb.com — Cisco warns of voice product security flaws.

Cisco on Thursday, January 22, warned of a default installation vulnerability in multiple voice products running on the IBM platform that leaves TCP and UDP ports open to malicious attack. Cisco said the security flaw could be exploited to cause denial-of-service attacks and administrative takeover. According to the Cisco advisory, the vulnerable voice products running on IBM servers install the Director Agent insecurely by leaving the service on port 14247 (both TCP and UDP) accessible without requiring user authentication. In addition to leaving the products susceptible to administrative takeover, a malicious attacker could make the IBM Director Agent process consume a server's entire CPU resources by scanning it with a network scanner. This advisory underscores the risks that come with the growing dependence on IP-based networks, especially in the enterprise. Specific information on this advisory can be found at:

http://www.cisco.com/warp/public/707/cisco-sa-20040121-voice.shtml

Category 23.7 VoIP

### 2004-05-18 VoIP voice over IP Internet telephony

http://www.nytimes.com/2004/05/18/technology/18voice.html?th=&pagewanted =print&position=

IBM and Cisco announced their intention to expand their VoIP (Voice over IP) Internet telephony services. VoIP offers increased functionality such as video-conferencing.

[MK notes: expect a whole new realm of hacking / phreaking to arise as VoIP spreads. Shall we call it phacking? As in, "Stop phacking around with my phone calls?"]

Category 23.7 VoIP

### 2004-05-24 VoIP Voice over IP Internet telephony Juniper Research study

DHS IAIP Daily; http://www.theregister.co.uk/2004/05/24/voip\_market\_boom/

May 24, The Register (UK) — VoIP to transform telecoms market.

Internet telephony will make up 12 percent of all telephony revenues in five years time, according to a study by analysts Juniper Research published Friday, May 21. Juniper claims the VoIP (Voice over Internet Protocol) market will contribute \$32 billion, out of a total telephony market worth approximately \$260 billion, by 2009. Service providers face the challenge of balancing new VoIP revenues against declines in their traditional fixed- line revenues, as flat- rate IP- based voice tariffs replace time and distance related charges. These changes will benefit more nimble service providers. According to Juniper, initial residential use of VoIP will be via a 'PSTN- bypass' through a PSTN interconnect - - this excludes free PC- to- PC or peer- to- peer services that do not offer PSTN interconnect. However in the longer term voice will be offered as part of a service bundle that includes email, Internet access and video telephony. In the enterprise, calls from IP- VPNs (virtual private networks) will also grow quickly as companies take advantage of network convergence to reduce costs. The study is available online: http://www.juniperresearch.com

Category 23.7 VoIP

2004-06-10 British Telecom circuit-switched network voice over IP VoIP

NewsScan

BT TO SHUT DOWN 'CIRCUIT-SWITCHED' NETWORK IN FAVOR OF VOIP

U.K. giant British Telecom will gradually shut down its traditional circuit-switched network and migrate over to technologies that route phone calls over the Internet. The change "will deliver our vision of a converged, multimedia world where our customers can access any communications service from any device, anywhere -- at broadband speed," says BT Wholesale CEO Paul Reynolds. The new system will enable each subscriber to have a single phone number for both mobile and fixed-line services, and will make possible such add-on features as family conference calls, video streaming and voice-activated phones. BT estimates that by the 2008-09 fiscal year, the new network could save it about £1 billion annually. (AP 10 June 2004)

Category 23.7 VoIP

#### voice over IP VoIP US consumer use research

2004-06-28 NewsScan

VOIP CATCHING ON

More than 25% of Internet users in the U.S. are aware of VoIP (voice over Internet Protocol) telephony, and 13% of those have considered switching over to Internet telephony for their residential phone service. The new figures from a study conducted by the Pew Internet & American Life

Project and the New Millennium Research Council also show that 11% of Internet users (14 million Americans) have actually made some kind of VoIP phone call. "Anecdotal evidence suggests that the 'pioneering consumer' often faces new technology 'glitches,' but then reaps the benefits and

enjoys being the first on the block with a new gadget," says Pew senior research specialist John Horrigan. The findings suggest that it's not too soon for legislators to begin thinking about the implications of this new technology, says Allen Hepner, NMRC advisory board member: "This

'disruptive technology' is coming to all Americans; it is not a question of 'if,' but 'when.' VoIP also disrupts existing laws and regulations in the telecom arena. Legislators and regulators would be wise to reexamine existing policy sooner rather than later, so as to minimize regulatory uncertainties for business and consumers." (Pew Internet & American Life Project News Release 28 Jun 2004)

Category	23.7	VoIP	
----------	------	------	--

2004-07-06 voice-over-IP VoIP adoption obstacles AT&T

NewsScan

OBSTACLES TO NET PHONE SERVICE

AT&T says it expects to have 1 million customers for its voice-over-Internet-protocol (VoIP) phone service by the end of next year, and cable-TV company Comcast expects to offer VoIP all its customers by the end of 2006; however, Mark Main of the British consulting firm Ovum warns

that -- although everyone will be using VoIP 10 or 15 years from now -- the road to that point "will be quite varied, quite torturous and not at all clean." Some obstacles in the way: only 27% of U.S. online users have even heard of it; a VoIP subscriber needs a broadband connection, and phone service will be only as good as that broadband connection; prices may go up in the future due to increased regulation and taxes; and VoIP service, which depends on the regular power grid, will fail if grid should fail. (AP/San Jose Mercury News 6 Jul 2004)

Category 23.7	VoIP
2004-08-02	voice-over-IP VoIP hacking phreaking stealing theft service tapping eavesdropping voyeurism

NewsScan

**VOIP -- VOYEURISM OVER INTERNET PROTOCOL?** 

With businesses and individuals flocking to Internet telephony as a cheap alternative to pricey landline phones, hackers are discovering new opportunities for eavesdropping and making mischief. Tapping phones by hacking into servers and hard drives is much easier than conventional wiretapping and analysts say even though very few incidents have been reported to date, it's just a matter of time. "Once you are running an Internet phone network, all those threats you worry about in the data world will be transferred to the voice world," says one security consultant. "Voice over Internet phones are not in the spotlight of hackers yet, but in this voyeuristic world, if someone can listen in on people's conversations and get a thrill, they will." In addition, voice packets offer new

opportunities for disguising and distributing malignant code. "You can spoof a packet and insert myself into a communications flow," says a systems engineer for Mirage Networks. "This kind of threat has been around for a while for data, but now it will move into voice. As you see a broader

acceptance of voice over Internet, you'll see more spoofs." (New York Times 2 Aug 2004)

Category 23.7 VoIP

2004-08-02 hackers phone phreaking voice-over-IP VoIP corporate network attack

DHS IAIP Daily; http://www.nytimes.com/2004/08/02/technology/02virus.html

August 02, New York Times — Hackers are discovering a new frontier:

Internet telephone service. Internet phones break voice conversations into data packets and route them over the Internet, a cheap and more flexible alternative to traditional phone calls that travel over copper wires. But Internet phones and the routers and servers that steer and store the digitized calls are susceptible to bugs, viruses and worms. Already, a few malicious attacks have shut down corporate Internet phone networks, disrupting business at a cost of millions of dollars. With Internet phones, hackers or disgruntled employees with access to a company's phone server can eavesdrop on conversations by surreptitiously installing software that can track voice packets. In theory, hackers can listen in on anyone's conversation, including those of ordinary consumers using a commercial Internet phone service. Hackers, though, are more likely to focus on a business's Internet phone lines to glean information that can be used for profit. Anecdotal evidence and the history of trouble with data networks suggest that it is only a matter time before the number and seriousness of the attacks increases as more companies start digital phone systems and merge them with their data networks.

Category 23.7 VoIP

### 2004-08-02 voice-over-IP VoIP outage Vonage

DHS IAIP Daily; http://zdnet.com.com/2100- 1105\_2- 5293439.html

August 02, CNET News.com — VoIP provider Vonage suffers outage.

Net phone service provider Vonage confirmed that it suffered its first outage in 18 months on Monday, August 2, due to problems at partner Global Crossing. Customers could still receive calls, but a small percentage of Vonage's 200,000 total subscribers couldn't make outbound calls from around 7 a.m. to 8 a.m. PDT, at which time the problem was fixed. Vonage's Website was knocked off the Internet during that time as well, because Global Crossing also hosts the site, according to a Vonage representative. VoIP requires a broadband connection; calls don't dial directly to 911; and if power to a home or office is lost, so is phone service.

Category 23.7 VoIP

### 2004-08-24 Cisco Internet phone service voice-over-IP VoIP networking

NewsScan

CISCO SERIOUS ABOUT INTERNET PHONE SERVICE

Computer-networking giant Cisco Systems is acquiring P-Cube, a privately held maker of software for monitoring Internetprotocol network activity, to help Cisco offer service-providers additional products to manage such IP services as voice-over-Internet protocol (VoIP), interactive

gaming, and video-on-demand. (AP/USA Today 24 Aug 2004)

Category 23.7 VoIP

### 2004-10-07 Skype VoIP voice over IP

NewsScan; http://www.latimes.com/technology/la-fi-skype7oct07

SKYPE GOES CALLING ON BUSINESSES

Internet telephony service Skype Technologies is turning its attention to small- and medium-size businesses, hoping to duplicate its tremendous success with individual users. "We've been targeting Skype to the individual, not to the residential or business markets. But what we found in a recent survey is that 48% of our customers are people using it for business," says Skype co-founder Niklas Zennstrom. Skype uses filesharing technology to form its network on the fly -- similar to the way that Kazaa filesharing software works. That's no coincidence -- Skype co-founders Zennstrom and Janus Friis are also the original creators of Kazaa. Skype currently counts 12 million users worldwide and last month's introduction of Skype Out -- a service that enables users to make calls to recipients with regular phone service for a minuscule charge -- resulted in an additional 200,000 paying customers. And while up until now, Skype has been offered free, the company's new focus signals a change. "[Zennstrom] is migrating from free services. He's got a revenue plan," says one industry advocate.

# Category 23.7 VoIP 2004-11-08 VoIP voice over IP regulation oversight FCC Federal Communications Commission regulation federal jurisdiction

NewsScan; http://www.siliconvalley.com/mld/siliconvalley/10128196.htm

FCC TO STATES: LEAVE INTERNET PHONE OVERSIGHT TO US

The Federal Communications Commission is planning to declare Internet phone service off-limits to state regulators. Bruce P. Mehlman of the trade group Internet Innovation Alliance says: "The decision before the FCC is critical, and very serious. The question for regulators is: Do we treat it like telecommunications, taxing it and regulating it heavily, or like information technology, keeping our hands off and letting market-based innovation benefit everyone?" But Mark Cooper of the Consumer Federation of America disagrees, saying: "If you let these people avoid their public responsibilities and not pay their fair share for using the network, the people left behind are going to be harmed by rising prices and declining quality." (San Jose Mercury News 8 Nov 2004)

Category 23.7 VoIP

### 2004-11-22 Kazaa Skype VoIP voice over IP

NewsScan;

http://news.com.com/Kazaa+offers+unlimited+free+Internet+phone+calls/2110-7352\_3-5463440.html

KAZAA OFFERS FREE VOIP CALLS

The latest version of Kazaa software, distributed by Sharman Networks, incorporates Internet telephony software from Skype Technologies, which is also owned by Kazaa founders Niklas Zennstrom and Janus Friis. That means while people are downloading their music they can also make free online calls anywhere in the world. (Reuters/CNet. com 22 Nov 2004)

## 23.8 SMS

Category 23.8

airport airline security short message service SMS check-in passenger

2004-08-03 NewsScan

SINGAPORE AIRLINES INTRODUCES SMS CHECK-IN

SMS

Passengers on Singapore Airlines will now be able to check in for flights by sending a text message on their mobile phones. The short message service (SMS) function is the latest use of technology that Singapore Airlines has introduced to make checking in easier and quicker, adding to Internet, mobile phone and fax facilities. After checking in remotely, passengers need to pick up their boarding passes and check in their luggage on the day of departure from a dedicated counter, rather than wait in regular queues. (The Age 3 Aug 2004) rec'd from John Lamp, Deakin U.

## 24.2 Windows NT/2K/XP

 

 Category
 24.2
 Windows NT/2K/XP

 2004-02-16
 exploit vulnerability Microsoft ASN.1 operating systems Windows NT XP 2000 Trojan Horse

DHS IAIP Daily; http://www.gcn.com/vol1\_no1/daily- updates/24946- 1.html

February 16, Government Computer News - Exploit code for Microsoft vulnerability circulating.

Security researchers say code designed to exploit a recently announced critical vulnerability in Microsoft operating systems now is widespread on the Internet. The code crashes targeted computers by exploiting a flaw in Microsoft's Abstract Syntax Notation 1 Library in Windows NT, 2000 and XP. The exploit code was discovered Saturday, February 14, four days after the vulnerability and a patch to correct it was announced by Microsoft. The code is available on several discussion groups and Web sites. Ken Dunham of iDefense Inc. said there have been reports of denial- of- service attacks against specific targets using this exploit, but the attacks are not yet widespread. "It may be a few days before we see anything beyond a DOD attack," he said. "Several attackers are actively working on an ASN.1 exploit to spread Trojans and 'bots. One attacker has expressed an interest in creating a worm that will 'take down the Internet.'" Dunham said the malicious actors are capable of "weaponizing" the exploit, but have so far had little success in their tests. In other malicious- code news, Symantec Corporation has raised the security level for the new Welchia worm because of increasing numbers of infections. Welchia, also known as Nachi, first appeared last August in the wake of the MSBlaster worm. It automatically patched against the vulnerability exploited by Blaster. The new version, Welchia.b, appears to remove the MyDoom a and b worms from infected machines. Once installed on a machine, it tries successively to exploit three vulnerabilities against a random IP address.

Category 24.2 Windows NT/2K/XP

### 2004-03-10 Microsoft security bulletin vulnerability hole flaw patch fix Windows Media denialof-service

DHS IAIP Daily;

http://www.microsoft.com/technet/security/bulletin/ms04-009.mspx

March 09, Microsoft — Microsoft Security Bulletin MS04- 008: Vulnerability in Windows Media Services Could Allow a Denial of Service.

A vulnerability exists because of the way that Windows Media Station Service and Windows Media Monitor Service, components of Windows Media Services, handle TCP/IP connections. If a remote user were to send a specially- crafted sequence of TCP/IP packets to the listening port of either of these services, the service could stop responding to requests and no additional connections could be made. The service must be restarted to regain its functionality. Windows Media Unicast Service may also be affected by a successful attack against Windows Media Station Service if Windows Media Unicast Service is sourcing a playlist from Windows Media Station Service. In this case, Windows Media Unicast Service could stop functioning when it encounters the next item in the playlist. Microsoft has assigned a risk rating of "Moderate" to this issue and recommends that system administrators consider installing the security update.

Category 24.2 Windows NT/2K/XP

### 2004-04-13 Microft security bulletin update Windows critical Jet Database Engine buffer overflow

DHS IAIP Daily;

http://www.microsoft.com/technet/security/bulletin/ms04-014.mspx

April 13, Microsoft — Microsoft Security Bulletin MS04- 014 Vulnerability in the Microsoft Jet Database Engine Could Allow Code Execution.

A buffer overrun vulnerability exists in the Microsoft Jet Database Engine (Jet) that could allow remote code execution. An attacker who successfully exploited this vulnerability could take complete control of an affected system, including installing programs; viewing, changing, or deleting data; or creating new accounts that have full privileges. Microsoft recommends that customers install the update at the earliest opportunity.

### 2004-04-13 Micrsoft security bulletin update Windows critical

DHS IAIP Daily;

http://www.microsoft.com/technet/security/bulletin/ms04-011.mspx

April 13, Microsoft — Microsoft Security Bulletin MS04- 011: Security Update for Microsoft Windows.

This update resolves several newly- discovered vulnerabilities which are detailed on the Microsoft Website. An attacker who successfully exploited the most severe of these vulnerabilities could take complete control of an affected system, including installing programs; viewing, changing, or deleting data; or creating new accounts that have full privileges. Microsoft has assigned a risk rating of "Critical" to these issues and recommends that customers apply the update immediately.

Category 24.2 Windows NT/2K/XP

### 2004-04-13 Microft security bulletin update Windows critical RPC DCOM

DHS IAIP Daily;

http://www.microsoft.com/technet/security/bulletin/ms04-012.mspx

April 13, Microsoft — Microsoft Security Bulletin MS04- 012 Cumulative Update for Microsoft RPC/DCOM.

This update resolves several newly- discovered vulnerabilities in RPC/DCOM. Each vulnerability is documented on the Microsoft Website. An attacker who successfully exploited the most severe of these vulnerabilities could take complete control of the affected system. An attacker could then take any action on the affected system, including installing programs; viewing, changing, or deleting data; or creating new accounts that have full privileges. Microsoft has assigned a risk rating of "Critical" to this issue and recommends customers apply the update immediately.

Category 24.2 Windows NT/2K/XP

### 2004-04-22 Microsoft flaw hole vulnerability exploit

DHS IAIP Daily; http://www.us- cert.gov/current/current\_activity.html#pct

April 22, US- CERT — Exploit for Microsoft PCT vulnerability released.

Exploit code has been publicly released that takes advantage of a buffer overflow vulnerability in the Microsoft Private Communication Technology (PCT) protocol. The vulnerability allows a remote attacker to execute arbitrary code with SYSTEM privileges. US- CERT is aware of network activity that is consistent with scanning and/or exploit attempts against this vulnerability. Reports indicate increased network traffic to ports 443/tcp and 31337/tcp. The PCT protocol runs over SSL (443/tcp) and the known exploit code connects a command shell on 31337/tcp. Note that the exploit code could be modified to use a different port or to execute different code. This vulnerability is remedied by the patches described in Microsoft Security Bulletin MS04- 011:

http://www.microsoft.com/technet/security/bulletin/MS04-011. mspx

Category 24.2 Windows NT/2K/XP

### 2004-04-26 Windows critical hijack flaw vulnerability

DHS IAIP Daily; http://www.esecurityplanet.com/alerts/article.php/3345351

April 26, eSecurity Planet — 'Critical' Windows hijack flaw reported.

Security researchers have discovered a serious boundary error vulnerability in multiple versions of Microsoft's Windows platform and warned that attackers could hijack systems via Windows Explorer and Internet Explorer. Rodrigo Gutierrez, a researcher with Trustix AS, notified Microsoft of the flaw with a warning that it could be exploited by malicious attackers to cause a buffer overflow and lead to system takeover. Microsoft confirmed Gutierrez's findings and recommended users install the latest service packs for Windows XP and Windows 2000. Independent security consultants Securia said the vulnerability "has been confirmed on fully patched systems running Windows XP and Windows 2000." Securia urged Windows XP and Windows 2000 users to restrict traffic in border routers and firewalls as a temporary workaround. Users could also disable the "Client for Microsoft Networks" for network cards to impact file sharing functionality. The flaw also reportedly affects Windows 95, 98, and Me. Securia Advisory SA11482:

http://secunia.com/advisories/11482/

2004-04-26 Microsoft Windows vulnerability flaw hole exploit worm

DHS IAIP Daily; http://informationweek.securitypipeline.com/news/19201802;js essionid=LUENRK1IB4PBYQSNDBGCKHQ

April 26, InformationWeek — Windows vulnerability exploited, worm may be next.

Security experts are monitoring widespread use of exploit code that takes advantage of a recently- disclosed vulnerability in Windows, but a worm, although anticipated, hasn't yet been spotted. The vulnerability stems from a flaw in Windows Protected Communications Technology (PCT) v. 1.0, a packet protocol within Microsoft's SSL library. An April bulletin from Microsoft warned that an attacker could create a buffer overflow condition on vulnerable Windows servers, then follow that by inserting their own code into the system to take control. Windows XP and Windows Server 2003 systems are also vulnerable. The first form of the exploit code was discovered within days of the disclosure of the SSL vulnerability, added Ken Dunham of iDefense. Last week, that code was updated to include a "phone home" feature that allowed hackers using it to be notified when they'd compromised a server. Additional information is available in Microsoft Knowledge Base Article 187498: http://support.microsoft.com/default.aspx?scid=

http://support.microsoft.com:80/support/kb/articles/q187/4/98.asp&NoWebContent=1

Category 24.2 Windows NT/2K/XP

### 2004-04-26 attack exploit source code Microsoft MS LSASS buffer overflow

DHS IAIP Daily; http://www.computerworld.com/securitytopics/security/story/0,10801,92696,00.html

April 26, IDG News Service — Attack code surfaces for recent MS security hole.

Computer code that claims to exploit a recently disclosed hole in Microsoft products has surfaced on a French- language Website. The code can be used by a remote attacker to trigger a buffer overrun vulnerability in the Local Security Authority Subsystem (LSASS). The code was released on Saturday, April 24, according to the Website. It was unclear whether the exploit code works, but notes attached by its author say some modifications may be necessary before the code can be used by a remote attacker to compromise Windows machines. An attacker who could exploit the LSASS vulnerability could remotely attack and take total control of Windows 2000 and Windows XP systems, according to Microsoft. Unlike e- mail worms and viruses, no user interaction would be necessary to trigger the LSASS buffer overflow, according to Johannes Ullrich of the SANS Institute's Internet Storm Center. Microsoft released a patch for the LSASS vulnerability in Microsoft Security Bulletin MS04- 011: http://www.microsoft.com/technet/security/bulletin/MS04- 011. mspx

Category 24.2 Windows NT/2K/XP

2004-04-29 Microsoft SSL patch bug confirmation Windows 2K 2000

DHS IAIP Daily; http://www.eweek.com/article2/0,1759,1578752,00.asp

April 29, eWEEK — Microsoft confirms bug in SSL patch.

Microsoft Corp. has confirmed in a knowledge base article that its patch for a critical bug can cause some Windows 2000 systems to lock up and fail at boot time. The patch is for a particularly critical vulnerability of which experts have begun to see exploits in the last few days. The knowledge base article goes by the unusually long name: "Your computer stops responding, you cannot log on to Windows, or your CPU usage for the System process approaches 100 percent after you install the security update that is described in Microsoft Security Bulletin MS04- 011." The article also gives one specific example, where the Nortel Networks VPN client is installed and the IPSec Policy Agent is set to Manual or Automatic for the startup type. In such cases, the article suggests disabling the IPSec Policy Agent.

2004-05-11 Microsoft patch vulnerability security bulletin code execution attack

DHS IAIP Daily; http://www.microsoft.com/security/security\_bulletins/200405\_ windows.asp

May 11, Microsoft — Microsoft Security Bulletin MS04- 015: Vulnerability in Help and Support Center Could Allow Remote Code Execution.

A remote code execution vulnerability exists in the Help and Support Center because of the way that it handles HCP URL validation. If a user is logged on with administrative privileges, an attacker who successfully exploited this vulnerability could take complete control of an affected system, including installing programs; viewing, changing, or deleting data; or creating new accounts with full privileges. Users whose accounts are configured to have fewer privileges on the system would be at less risk than users who operate with administrative privileges. Microsoft recommends that customers install the update at the earliest opportunity.

|--|--|--|

2004-05-12 windows microsoft security flaw patch sofware PC XP Server 2003

NewsScan

NEW MICROSOFT WINDOWS SECURITY FLAW

Microsoft has identified and released a Windows software patch for a new flaw that could allow hackers to take control of a PC by luring users to a malicious Web site and getting them to take certain actions there. The security flaw affects the latest versions of Windows, including Windows XP, and software for networked computers such as Windows Server 2003. A user would be vulnerable to the security flaw only by visiting the attacker's Web site and performing several actions there. (Reuters/USA Today 12 May 2004)

Category 24.2 Windows NT/2K/XP

### 2004-08-19 network time synchronization protocol NTP Microsoft operating systems Active Directory vulnerability time spoofing attacks

DHS IAIP Daily; http://www.securityfocus.com/bid/10980

August 19, SecurityFocus — Microsoft NTP time synchronization spoof weakness.

The NTP implementation in Microsoft operating systems is vulnerable to time spoofing attacks. An attacker may be able to alter the time on the domain controller, causing the entire domain to synchronize with the attacker specified time. This weakness may allow a malicious user to deny service to legitimate users, as correct time is required for many operations, including domain authentication and X.509 certificate expiration times. This weakness is reported to exist in all versions of Microsoft operating systems that include Active Directory support. Microsoft has implemented a default failsafe for time synchronization that prevents an attacker from adjusting the time for more than 12 hours. By setting this to a smaller amount, an attacker would have to spend more time altering the clock by significant amounts.

Category 24.2 Windows NT/2K/XP

### 2004-08-19 Microsoft Windows XP SP2 bugs vulnerability shell folder

DHS IAIP Daily; http://www.eweek.com/article2/0,1759,1637596,00.asp

August 19, eWEEK — Bugs, exploits dog XP SP2.

Microsoft has issued a hotfix for Windows XP Service Pack 2 to solve a problem about which many users have complained: programs that attempt to connect to loopback addresses other than 127.0.0.1 get error messages. However, since it is a hotfix, it is not fully supported. It is expected that Microsoft will issue a more permanent fix in the future. Meanwhile, security researchers are reporting a new vulnerability in SP2 that could allow a malicious Website to deposit an attack program on a user's system. The attack utilizes Internet Explorer's drag- and- drop features and the Windows "shell folders" to copy an executable from a malicious Website to a user's startup folder, from which it would execute the next time the user logged on. Secunia, a security consulting firm, said the attack works on a fully patched Windows XP Service Pack 1 system, and that the drag- and- drop approach could be replaced with a single click. For the attack to succeed, the user would have to visit a Website that hosted it and follow the instructions. Any attack code deposited would be scanned by anti- virus software on the user's computer.

### 2004-08-30 Microsoft Windows XP Service Pack 2 SP2 security update

DHS IAIP Daily; http://www.uscert.gov/cas/alerts/SA04- 243A.html

August 30, US- CERT — Cyber Security Alert SA04- 243A: Security Improvements in Windows XP Service Pack 2.

Windows XP Service Pack 2 is a major operating system update that contains a number of new security updates and features. Like other Microsoft Service Packs, Windows XP Service Pack 2 also includes previously released security fixes and other operating system updates. To help protect your Windows XP computer from attacks and vulnerabilities, install Service Pack 2 using Windows Update or Automatic Updates. Service Pack 2 makes significant changes to improve the security of Windows XP, and these changes may have negative effects effects on some programs and Windows functionality. Before you install Service Pack 2, back up your important data and consult your computer manufacturer's web site for information about Service Pack 2. Downloads available at: http://www.microsoft.com/windowsxp/sp2/default.mspx

Category 24.2 Windows NT/2K/XP

### 2004-09-17 Microsoft patch fix early warning systems customers

NewsScan

PATCH DEALS FAVOR BIG BUSINESS

Microsoft has quietly begun giving some of its largest customers early warning of what types of security patches it will be releasing. Under the free program, some customers are receiving three business days' notice as to how many security fixes Microsoft plans to release in its regular monthly bulletins, and which Microsoft products are affected. Customers also can learn how severe a threat the flaws pose several days before the general public gets that information. Microsoft began testing the program last year, and expanded it in April. It has not been widely publicized, and Microsoft has been offering the service to some customers individually through sales representatives. (The Australian 17 Sep 2004) Rec'd from John Lamp, Deakin U.

Category 24.2 Windows NT/2K/XP

### 2004-11-27 Microsoft WINS packet memory overwrite vulnerability code execution attack

DHS IAIP Daily; http://www.securitytracker.com/alerts/2004/Nov/1012341.html

November 27, SecurityTracker — Microsoft WINS Memory overwrite lets remote users execute arbitrary code.

It is reported that a remote user can send a specially crafted WINS packet to the target server on TCP port 42 to modify a memory pointer and write arbitrary contents to arbitrary memory locations. This could permit a remote user to execute arbitrary code on the target system. There is no solution at this time.

# Category 24.2 Windows NT/2K/XP 2004-12-07 Microsoft Windows 2000 2K XP Resource Kit buffer overflow vulnerability no update issued

DHS IAIP Daily; http://www.securitytracker.com/alerts/2004/Dec/1012435.html

December 07, SecurityTracker — Microsoft Windows Resource Kit buffer overflow and input validation holes.

Several vulnerabilities were reported in the 'w3who.dll' Microsoft ISAPI extension in the Windows 2000/XP Resource Kit. A remote user can execute arbitrary code on the target system because the software does not properly validate user- supplied input before displaying HTTP headers or error messages. A remote user can create a specially crafted URL that, when loaded by a target user, will cause arbitrary scripting code to be executed by the target user's browser. No solution is available at this time.

Category 24.2 Windows NT/2K/XP

### 2004-12-14 Microsoft security patches update release December 2004 Wordpad DHCP HyperTerminal Windows Kernel LSASS WINS

DHS IAIP Daily; http://www.microsoft.com/technet/security/current.aspx

December 14, Microsoft — Microsoft releases December security updates.

Microsoft released five security updates on Tuesday, December 14. Vulnerable products are Wordpad, DCHP, HyperTerminal, Windows Kernel and LSASS, and WINS. Successful exploitation of the vulnerabilities in these products could allow a malicious user to execute remote code, launch a denial of service, or gain elevated privileges. Microsoft has assigned a risk rating of "Important" to these issues and recommends users install updates as soon as possible.

### 2004-12-22 EU Microsoft antitrust media player

NewsScan; http://www.washingtonpost.com/wp-dyn/articles/A18543-2004Dec22.html

EU COURT RULES AGAINST MICROSOFT

A European Union judge today ruled that Microsoft must immediately submit to sanctions imposed by EC regulators after they found that Microsoft broke antitrust laws by integrating its Windows Media Player into Windows, thus putting rival media software companies at a disadvantage. Microsoft had appealed the initial decision, arguing that pulling Media Player out of Windows would degrade its performance, but in today's ruling, Chief Judge Bo Vesterdorf of the Court of First Instance found that postponing sanctions would give Microsoft time to strengthen its grip on the market for media playing applications. Microsoft must now create two versions of Windows for European distribution -- one that contains Media Player and one without. Microsoft announced it would comply while contemplating its next legal move. (Washington Post 22 Dec 2004)

### Category 24.2 Windows NT/2K/XP

2004-12-24 Microsoft Windows unpatched holes warning Symantec heap overflow vulnerability no update issued

DHS IAIP Daily; http://www.computerworld.com/securitytopics/security/holes/s tory/0,10801,98532,00.html

December 24, IDG News Service — Researchers warn of multiple unpatched Windows holes.

The antivirus company Symantec Corp. warned its customers about a number of critical holes in Microsoft Corp.'s Windows operating system that surfaced late Thursday, December 23, that could make Windows systems vulnerable to compromise by remote attackers. Symantec acted after security researchers published the details of the heap overflow vulnerabilities in messages posted to online security news groups, including the Bugtraq mailing list and on xfocus.net. The flaws affect most supported versions of Windows, but Microsoft has not yet issued a patch for the newly disclosed holes. Windows users are vulnerable to Internet based attacks until patches are issued, Symantec said. Symantec recommended that Windows users exercise caution when receiving and opening files from unknown sources.

# Category 24.2 Windows NT/2K/XP 2004-12-28 Microsoft Windows kernel file parsing denial of service DoS vulnerability XP SP2 not vulnerable

DHS IAIP Daily;

http://security-protocols.com/modules.php?name=News&file=art icle&sid=2357

December 28, Security Protocols — Microsoft Windows Kernel ANI file parsing crash and denial of service.

Parsing a specially crafted ANI file causes the Windows kernel to crash or stop to work properly. An attacker can crash or freeze a target system if he sends a specially crafted ANI file within an HTML page or within an e- mail. Two vulnerabilities exist in the Windows kernel when it parses ANI files. These vulnerabilities are due to improper input validation of the frame number set and the rate number set in the ANI file header. Windows XP SP2 is not vulnerable.

## 24.3 UNIX flavors

Category 24.3 UNIX flavors

### 2004-01-07 Linux security flaw critical vulnerability warning virtual memory

NIPC/DHS; http://www.pcworld.com/resource/printable/article/0,aid,1140 88,00.asp

January 05, PC World — Security group warns of Linux flaw.

There is a critical vulnerability in the code used to manage virtual memory on Linux systems. The vulnerability affects versions of the Linux kernel up to and including version 2.6 and would give low-level Linux users total control over a Linux system. ISEC Security Research said Monday, January 5, that the problem is in kernel code for a component called "mremap," the core of the Linux operating system that provides basic services for all other parts of the operating system such as allocating processor time for the programs running on the computer and managing the system's memory or storage. Attackers could use the vulnerability to create an invalid virtual memory area, which could destabilize the Linux operating system or allow a malicious user to run attack code on the system. Attackers would need local user access to the vulnerable machine, but would not need any special privileges on the Linux system to exploit the hole, ISEC said. ISEC said they have developed test code to exploit the mremap vulnerability. Users should fix vulnerable systems as soon as software patches became available from their vendor. The original advisory is available here:

http://isec.pl/vulnerabilities04.html

Category 24.3 UNIX flavors

### HP Tru64 UNIX operating system vulnerability flaw patch fix

2004-01-20 NIPC/DHS;

http://news.zdnet.co.uk/software/linuxunix/0,39020390,39119149,00.htm

January 16, ZDNet — HP patches critical security holes in Tru64 Unix.

Critical security vulnerabilities in HP's Tru64 Unix operating system were patched on Friday, January 16, after it was discovered that implementations of IPsec and SSH programs, which carry VPN and secure system command traffic, were vulnerable to attackers. The vulnerabilities both were found in vital components of the operating system and both could enable malicious users to either take control of a machine or launch a denial of service attack. SSH, a secure Telnet program, is used to securely send commands to a server, while IPSec is used to create virtual private networks to carry encrypted information over the Internet between two computers. HP has issued patches that will fix any known problems. Only HP's Tru64 UNIX 5.1B is affected and fixes for both the IPsec software and SSH software can be found on HP's Web site: http://us-support3.external.hp.com/common/bin/doc.pl/sid=485 45bf71719ae72bf

Category 24.3 UNIX flavors

### 2004-01-20 HP Tru64 UNIX operating system vulnerability flaw patch fix

DHS IAIP Daily; http://news.zdnet.co.uk/software/linuxunix/0,39020390,391191 49,00.htm

January 16, ZDNet — HP patches critical security holes in Tru64 Unix.

Critical security vulnerabilities in HP's Tru64 Unix operating system were patched on Friday, January 16, after it was discovered that implementations of Ipsec and SSH programs, which carry VPN and secure system command traffic, were vulnerable to attackers. The vulnerabilities both were found in vital components of the operating system and both could enable malicious users to either take control of a machine or launch a denial of service attack. SSH, a secure Telnet program, is used to securely send commands to a server, while IPSec is used to create virtual private networks to carry encrypted information over the Internet between two computers. HP has issued patches that will fix any known problems. Only HP's Tru64 UNIX 5.1B is affected and fixes for both the Ipsec software and SSH software can be found on HP's Web site: http://us- support3.external.hp.com/common/bin/doc.pl/sid=485 45bf71719ae72bf

### 2004-01-22 Linux security certified IBM Novell SuSE

NewsScan

CERTIFICATION GIVE A BOOST TO LINUX IN GOV'T CONTRACTS

IBM and Novell's SuSE Linux have won a security certification for their combined systems, an achievement indicating that their products have been tested against strict standards — including security capabilities. IBM executive James Sterlings says, "This further underscores government confidence in Linux." (VNUnet News 22 Jan 2004)

Category 24.3 UNIX flavors

### 2004-01-23 OSAIA Linux security threat SCO

NewsBits;

http://www.computerweekly.com/articles/article.asp?liArticleID=127789

Linux threatens US security, SCO tells Congress

The SCO Group has confirmed that it sent a letter to all 535 members of the US Congress which claimed that Linux and opensource software is a threat to the security and economy of the US. The letter, dated 8 January, was published on the internet this week by an open-source lobbying organisation called the Open Source and Industry Alliance (OSAIA). The letter states that the commoditising influence of open-source software such as Linux is bad for the US economy and argues that open source also skirts export controls governing commercial products.

Category 24.3 UNIX flavors

### 2004-02-18 Sun Cobalt server security holes vulnerability update issued

DHS IAIP Daily;

http://searchsecurity.techtarget.com/originalContent/0,289142,sid14\_gci950995,00. html?track=NL- 358

February 18, SearchSecurity.com — Sun combats security holes in cancelled Cobalt line.

Sun Microsystems continues to battle operating system vulnerabilities in its doomed line of Cobalt appliance servers. Administrators should upgrade to prevent remote exploits that could include cracking private keys, exposing confidential data, spoofing identities, escalating privileges, executing arbitrary code and denial of service. Perhaps the most serious vulnerability is a heap- based buffer overflow in rsync. Remote attackers can use this to gain access to a system or execute arbitrary code. Sun has fixes for RaQ 550, Qube 3 and RaQ 4. A defect in gnupg incorrectly creates El Gamal sign and encrypt keys using the same key component. This could allow an attacker to get the private key from a signature, which could be used to spoof identities and decrypt confidential data. Fixes are available for Qube 3, RaQ 550 and RaQ XTR. An integer overflow in the ls program in the fileutils or coreutils packages can render applications that use ls, including wu- ftpd, vulnerable to remote exploitation. Attackers could cause a denial of service on the server. There are fixes for RaQ XTR, RaQ 550, Qube 3 and RaQ 4. Finally, an update is available for an unspecified vulnerability in IPtables on RaQ 550.

Category 24.3 UNIX flavors

### 2004-02-19 Linux kernel 2.4 server flaws vulnerabilities update issued

DHS IAIP Daily;

http://news.com.com/2100- 1002\_3- 5162055.html?tag=nefd\_top

February 19, CNET News.com — Linux servers at risk from trifecta of flaws.

Three separate security flaws could be used by an ordinary user to gain total control of a Linux server or workstation, security researchers have warned. Two of the vulnerabilities lie in the way the Linux kernel- - the core of the open- source operating system- - manages memory. They affect all current versions of Linux, according to advisories released on Wednesday by iSEC Security Research, a Polish security company. The third flaw affects the module for the kernel that supports ATI Technologies' Rage 128- bit video card. Because Linux is frequently used on shared servers, security holes that allow a user to expand their access rights on a computer are serious, said Alfred Huger of Symantec. However, they are not as critical as flaws that allow an outsider to compromise the computer, he said. The Linux Kernel Project released a new version of the 2.4 series kernel- - version 2.4.25- - to fix the vulnerability. Linux companies and projects that package their own version of Linux have rushed to deliver updates. Red Hat, Novell's SuSE Linux, Debian and other Linux distributions had released fixes by Thursday, February 19.

## Category24.3UNIX flavors2004-03-10security vulnerability flaw hole patch fix Linux privilege escalation denial-of-service<br/>Gentoo

### NIPC/DHS

March 09, eSecurity Planet — Linux privilege escalation hole detected.

According to an advisory from computer security consultants iSEC Security Research, a flaw was found in the Linux kernel memory management code and is completely unrelated to a similar vulnerability reported in February. The flaw carries a "critical" rating and affects Linux versions 2.2 up to and including 2.2.25; it also impacts versions 2.4 up to and including 2.4.24 as well as versions 2.6 up to and including 2.6.2. "Proper exploitation of this vulnerability leads to local privilege escalation giving an attacker full super- user privileges. The vulnerability may also lead to a denial- of- service attack on the available system memory," iSEC warned. Linux distributor Gentoo confirmed its implementation of the open source operating system was susceptible to the flaw and strongly urged uses to upgrade to newer, more secure versions. The flaw was discovered in the memory subsystem which allows for shrinking, growing, and moving of chunks of memory along any of the allocated memory areas which the kernel possesses. iSEC Security Research found that the code doesn't check the return value of the memory function.

Category 24.3 UNIX flavors

### 2004-04-16 Linux open-source operating system kernel flaws

DHS IAIP Daily; http://www.esecurityplanet.com/trends/article.php/3341341

April 16, eSecurity Planet — Multiple Linux flaws reported.

Security researchers are warning of a buffer overflow security flaw in the Linux kernel that can be exploited to lead to privilege escalation attacks. According to an advisory issued by iDEFENSE, the vulnerabilities affect Linux Kernel 2.6.x; Linux Kernel 2.5.x and Linux Kernel 2.4.x. The company found that affected versions of Linux kernel performed no length checking on symbolic links stored on an ISO9660 file system, a problem that allows a malformed CD to perform an arbitrary length overflow in kernel memory. "Symbolic links on ISO9660 file systems are supported by the 'Rock Ridge' extension to the standard format. The vulnerability can be triggered by performing a directory listing on a maliciously constructed ISO file system, or attempting to access a file via a malformed symlink on such a file system. Many distributions allow local users to mount CDs, which makes them potentially vulnerable to local elevation attacks," according to the security alert. Updated Linux kernel versions are available at kernel.org. Separately, security firm Secunia warned of an information leak and denial- of- service holes in Linux Kernel 2.4.x and 2.6.x. The information leak problem was discovered with the ext3, XFS, and JFS file system code and can lead to the exposure of data like cryptographic keys to malicious attackers. Another error was found within the OSS code for SoundBlaster 16 devices that could be used to trigger denial- of- service attacks with odd numbers of output bytes are submitted.

Category 24.3 UNIX flavors

### 2004-05-03 Linux operating systems vulnerabilities security

DHS IAIP Daily; http://www.fcw.com/fcw/articles/2004/0503/feat-linux3-05-03-04.asp

May 03, Federal Computer Week — Linux has its own security holes.

There may be fewer viruses designed to attack the Linux operating system, but experts warn that Linux is no more bulletproof than any other system. Agencies that adopt Linux should be aware of its vulnerabilities, according to Travis Witteveen, of security firm F- Secure Corp. "Computing systems are very similar, whether they're called Linux, Windows, Unix, MacIntosh, or even PocketPC," he said. Vius writers will target Linux when the system gains a high enough profile, Witteveen said. But even now, there are some Linux viruses out in cyberspace. The most damaging Linux virus so far, the Slapper worm, infected 20,000 systems in 100 countries in late 2002, said Laura DiDio, senior analyst of application infrastructure and software platforms for the Yankee Group. "That pales in comparison to the most damaging Windows virus, MyDoom and its variants, which infected several million computers in three weeks," she said. Linux is "on everyone's radar screen," and creators of malicious code are increasingly taking notice, she said. Many Linux viruses don't require user interaction, unlike most Windows attacks that depend on the user to run an attached file in order to infect the computer.

## Category24.3UNIX flavors2004-06-28Project Looking Glass Sun Microsystems 3-D interface software

NewsScan

SUN 3-D INTERFACE OFFERED TO OPEN-SOURCE COMMUNITY

Sun Microsystems has designed 3-D interface software to compete with the PC desktop metaphor of desktops and file folders. The new technology will be offered to the open source community, and a Sun executive says, "What we want to do is leverage the community of open-source developers to do things we might not have thought of." Produced through a company effort dubbed Project Looking Glass, the 3D interface allows windows containing documents or images to be turned sideways (like books on a shelf) and spun around so that notations can be made on the reverse side. It may eventually be used on Windows machines, but Sun is initially planning to use the

technology on desktop machines running Linux or Sun's own Solaris operating system. Sun president and COO Jonathan Schwartz says that Project Looking Glass reflects a swing in software development back toward desktop machines or other client devices, instead of running programs on centralized servers. (Wall Street Journal 28 Jun 2004)

Category 24.3 UNIX flavors

### 2004-07-29 Gentoo Linux Samba vulnerability fix patch update SWAT buffer overflow

DHS IAIP Daily; http://searchsecurity.techtarget.com/originalContent/0,28914 2,sid14\_gci996615,00.html

July 29, SearchSecurity.com — Gentoo fixes Samba vulnerabilities.

Gentoo Linux has fixed buffer overflow vulnerabilities in Samba. The buffer overflow found in SWAT is located in the base64 data decoder used to handle http basic authentication. The same flaw is present in the code used to handle the sambaMungedDial attribute value when using the ldapsam passdb backend. Another buffer overflow was found in the code used to support the 'mangling method = hash' smb.conf option. The SWAT authentication overflow could be exploited to execute arbitrary code with the rights of the Samba daemon process. The overflow in the sambaMungedDial handling code is not thought to be exploitable. The buffer overflow in 'mangling method = hash' code could also be used to execute arbitrary code on vulnerable configurations. For a workaround, the Gentoo advisory suggests users disable SWAT, not use ldapsam passdb backends and avoid the 'mangling method = hash' option. All Samba users should upgrade to the latest version, Gentoo said: http://www.gentoo.org/security/en/glsa/glsa- 200407- 21.xml

Category 24.3 UNIX flavors

### 2004-07-30 Oracle database privilege escalation vulnerability UNIX Linux

DHS IAIP Daily; http://www.securityfocus.com/bid/10829

July 30, SecurityFocus — Oracle database default library directory privilege escalation vulnerability. Oracle database implementations are reportedly prone to a default library directory privilege escalation vulnerability. This issue arises due to a default configuration error that will permit the attacker to replace libraries required by setuid root applications with arbitrary code. This issue would allow an Oracle software owner to execute code as the superuser, taking control of the entire system. It should be noted that this vulnerability only affects Oracle on UNIX/Linux platforms. SecurityFocus is currently not aware of any vendor- supplied patches for this issue.

Category 24.3 UNIX flavors

### 2004-08-03 Citadel UX buffer overflow vulnerability denial of service DoS

DHS IAIP Daily; http://secunia.com/advisories/12197/

August 03, Secunia — Citadel/UX "USER" Command Buffer Overflow Vulnerability.

A vulnerability in Citadel/UX can be exploited by malicious people to cause a DoS (Denial of Service) and potentially compromise a vulnerable system. The vulnerability is caused due to boundary error within the citadel service when processing "USER" commands. This can be exploited to cause a stack- based buffer overflow by passing an overly long argument (about 94 bytes) to the "USER" command. Successful exploitation may allow execution of arbitrary code. The vulnerability has been reported in version 6.23 and prior.

### 2004-08-04 Linux vulnerability pointer handling kernel memory disclosure

DHS IAIP Daily; http://secunia.com/advisories/12210/

August 04, Secunia — Linux kernel file offset pointer handling memory disclosure vulnerability.

A vulnerability in the Linux kernel can be exploited by malicious, local users to disclose sensitive information in kernel memory. The vulnerability is caused due to race conditions and conversion errors when handling 64- bit file offset pointers. Successful exploitation may disclose large portions of kernel memory. The vulnerability has been reported in version 2.4.26 and prior and in version 2.6.7 and prior. Users should grant only trusted users access to affected systems.

Category 24.3 UNIX flavors

### 2004-08-04 YaST2 SuSE Linux shell code injection vulnerability update patch

DHS IAIP Daily; http://www.securityfocus.com/bid/10867/info/

August 04, SecurityFocus — YaST2 utility library file verification shell code injection vulnerability.

YaST2 utility library 'liby2util' is affected by a file verification shell code injection vulnerability. This issue is due to a design error that fails to properly validate files. An attacker could leverage this issue to inject malicious shell code into a file name being transferred using the vulnerable utility. This might facilitate privilege escalation and unauthorized access. S.u.S.E. has made updated binaries available on their FTP sites.

Category 24.3 UNIX flavors

### 2004-08-09 HP Tru64 UNIX Mozilla libpng vulnerabilities

DHS IAIP Daily; http://secunia.com/advisories/12240/

August 09, Secunia — Mozilla Application Suite for Tru64 UNIX libpng Vulnerabilities.

HP has confirmed some vulnerabilities in the Mozilla Application Suite for Tru64 UNIX, which can be exploited by malicious people to cause a DoS (Denial of Service) or compromise a vulnerable system. The vulnerabilities affect versions prior to 1.7. Users should install Mozilla Application Suite for HP Tru64 UNIX V1.7. http://h30097.www3.hp.com/internet/download.htm

Category 24.3 UNIX flavors

### 2004-08-11 Sun Solaris X Display Manager XDMCP request vulnerability remote protocol

DHS IAIP Daily; http://www.kb.cert.org/vuls/id/139504

August 11, US- CERT — Vulnerability Note VU#139504: Sun Solaris X Display Manager does not properly handle invalid XDMCP requests.

The X Display Manager (xdm(1)) is responsible for managing collections of X displays from local or remote servers using the X Display Manager Control Protocol (XDMCP). The Sun Solaris X Display Manager contains a denial- of- service vulnerability that could be triggered by an invalid XDMCP packet. A remote attacker with the ability to send XDMCP packets to a vulnerable system could cause the X Display Manager to crash. For more information on patches available for your system, please refer to Sun Security Alert 57619: http://sunsolve.sun.com/pub- cgi/retrieve.pl?doc=fsalert/57619

Category 24.3 UNIX flavors

### 2004-08-16 SuSE Linux operating system rsync program vulnerability Red Hat Package Manager rpm update issued

DHS IAIP Daily; http://www.suse.com/de/security/2004\_26\_rsync.html

August 16, SUSE, Inc. — SUSE Linux rsync vulnerability.

If rsync is running in daemon- mode and without a chroot environment it is possible for a remote attacker to trick rsyncd into creating an absolute pathname while sanitizing it. As a result it is possible to read/write from/to files outside the rsync directory. SUSE Linux 8.1, 8.2, 9.0, and 9.1 are vulnerable. Please download the update package for your distribution and verify its integrity by the methods listed in section three of this announcement. Then, install the package using the command "rpm - Fhv file.rpm" to apply the update. Our maintenance customers are being notified individually. The packages are being offered to install from the maintenance web.

### 2004-08-25 OpenBSD kernal panic attack ICMP request system reboot

DHS IAIP Daily; http://www.zone- h.org/advisories/read/id=5413

August 25, zone- h.org — OpenBSD kernel panic.

A vulnerability exists in OpenBSD 3.4 and 3.5 configured to act as a gateway. This vulnerability may cause the kernel to crash. An OpenBSD 3.5 machine, configured as a gateway, with active bridging, and the link2 option given (for IPSec processing), is vulnerable to a crash when to a single ICMP echo request sent from a machine on interface A's network is sent to a machine on interface B's network. No core file is generated. If the DDB\_PANIC option is set, the machine reboots upon receipt of the ICMP echo request. Patches are available at: ftp://ftp.openbsd.org/pub/OpenBSD/patches

Category 24.3 UNIX flavors

## 2004-09-02 Linux 2.6 kernel open source operating system panic integer overflow vulnerability XDR decode functions update issued

DHS IAIP Daily; http://www.securitytracker.com/alerts/2004/Sep/1011138.html

September 02, SecurityTracker — Linux Kernel integer overflow in kNFSd lets remote users panic the system.

An integer overflow vulnerability exists in the Linux kernel in kNFSd. A remote user can cause the target system to crash. SuSE reported that there are various "signedness issues and integer overflows" in the kNFSd and the XDR decode functions in the Linux 2.6 kernel. A fix is available for the kNFSd overflow in the upstream 2.6.9- rc1 kernel version.

Category 24.3 UNIX flavors

### 2004-11-10 Linux kernel loader vulnerability root access arbitrary code execution attack

DHS IAIP Daily; http://www.securitytracker.com/alerts/2004/Nov/1012165.html

November 10, SecurityTracker — Linux Kernel binfmt\_elf Loader lets local users obtain root access.

A local user can execute arbitrary code with setuid privileges to obtain root access on the target system. Several flaws have been discovered in the ELF loader in the processing of set user id (setuid) binaries. There is no solution at this time.

Category 24.3 UNIX flavors

### 2004-11-19 FreeBSD fetch utility integer overflow vulnerability

DHS IAIP Daily; http://secunia.com/advisories/13226/

November 19, Secunia — FreeBSD fetch utility integer overflow vulnerability.

A vulnerability has been reported in FreeBSD which potentially can be exploited by malicious people to compromise a user's system. The vulnerability is caused due to an integer overflow in the fetch utility when processing HTTP headers. This can be exploited to cause a buffer overflow by returning a specially crafted response. Successful exploitation may allow execution of arbitrary code, but requires that a user is tricked into connecting to a malicious Web server. Original advisory and updates are available at: ftp://ftp.freebsd.org/pub/FreeBSD/CERT/advisories/FreeBSD- SA- 04:16.fetch.asc

Category 24.3 UNIX flavors

### 2004-11-30 Linux kernel datagram serialization error user privilege escalation update issued

DHS IAIP Daily; http://www.securitytracker.com/alerts/2004/Nov/1012363.html

November 30, SecurityTracker — Linux Kernel datagram serialization error may let local users gain elevated privileges.

A local user may be able to obtain elevated privileges because the kernel does not properly serialize received datagrams. A local user can exploit this flaw to modify kernel space memory and potentially obtain elevated privileges. A fix is available in 2.4.28 and via BitKeeper at: http://linux.bkbits.net:8080/linux- 2.4/cset@4199284dnTPrPLR- yhP\_rOBHXJlltA

### 2004-12-02 IBM AIX privilege escalation vulnerabilities code execution attack update issued

DHS IAIP Daily; http://secunia.com/advisories/13589/

December 02, Secunia — IBM AIX multiple privilege escalation vulnerabilities.

Four vulnerabilities have been reported in AIX, which can be exploited by malicious, local users to gain escalated privileges. These vulnerabilities are due to errors in the paginit utility, the "/bin/Dctrl" utility, the uname utility, and the grep utility. Successful exploitation of the vulnerabilities allows execution of arbitrary code with "root" privileges. Apply APARs: http://www- 912.ibm.com/eserver/support/fixes/fcgui.jsp

# Category 24.3 UNIX flavors 2004-12-03 AIX operating system startup script vulnerability Object Data Manager ODM update issued

DHS IAIP Daily; http://secunia.com/advisories/13370/

December 03, Secunia — AIX unspecified system startup scripts vulnerability.

A vulnerability has been reported in AIX, which can be exploited by malicious, local users to inject arbitrary data into the ODM (Object Data Manager) or cause a vulnerable system to hang during boot. The vulnerability is caused due to an unspecified error within the system startup scripts. Apply APARs available at: http://www-912.ibm.com/eserver/support/fixes/fcgui.jsp

Category 24.3 UNIX flavors

### 2004-12-13 Linux flaws Microsoft security research reliability security open-source

NewsScan;

http://news.com.com/Security+research+suggests+Linux+has+fewer+flaws/2100 -1002\_3-5489804.html

REPORT CONCLUDES LINUX HAS FEWER FLAWS

A four-year research effort by code-analysis firm Coverity has concluded that Linux has significantly fewer software bugs in it than most commercial counterparts. Coverity uncovered 985 flaws in the 5.7 million lines of code that make up the Linux core operating system, compared with the more than 5,000 defects typically found in commercial software of similar size. "Linux is a very good system in terms of bug density," says Coverity CEO Seth Hallem. Though Coverity's report doesn't contain any specific data about the frequency of glitches in Microsoft's Windows operating system, it's likely to add fuel to the debate over which system -- Linux, Mac OS or Windows -- is most secure. One recent report found that Red Hat Linux contained fewer critical flaws than Microsoft Windows, while a Forrester Research study (sponsored by Microsoft) unsurprisingly favored Microsoft. (CNet News.com 13 Dec 2004)

Category 24.3 UNIX flavors

## 2004-12-21 Hewlett-Packard HP UX ftpd file transfer protocol daemon buffer overflow vulnerability update issued

DHS IAIP Daily;

http://www.idefense.com/application/poi/display?id=175&type= vulnerabilities

December 21, iDEFENSE — Hewlett Packard HP- UX ftpd remote buffer overflow vulnerability.

Remote exploitation of a buffer overflow vulnerability in the file transfer protocol (FTP) daemon included in multiple versions of Hewlett- Packard Development Co.'s (HP) HP- UX allows attackers to gain remote root access in certain configurations. The severity of this issue is mitigated by the fact that in most production environments, administrators will not be using the debug- logging feature of FTP daemon. Apply patches: http://www.itrc.hp.com/service/patch/mainPage.do

## 2004-12-26 SHOUT cast software filename format string vulnerability DNAS Linux HTTP request no update issued

DHS IAIP Daily; http://secunia.com/advisories/13661/

December 26, Secunia — SHOUTcast filename format string vulnerability.

A vulnerability in SHOUTcast DNAS/Linux version 1.9.4 has been reported which can be exploited by malicious people to compromise a vulnerable system. The vulnerability is caused due to a format string error in the URL handling within the processing of requested filenames. This can be exploited to execute arbitrary code by sending a specially crafted HTTP request containing format specifiers. No vender solution is available at this time.

## **24.4 TCP/IP & HTTP**

Category 24.4 TCP/IP & HTTP

### Microsoft security bulletin patch flaw vulnerability fix Exchange Server http

DHS/IAIP Update

2004-01-14

MICROSOFT SECURITY BULLETIN MS04- 002: VULNERABILITY IN EXCHANGE SERVER 2003 COULD LEAD TO PRIVILEGE ESCALATION.

A vulnerability exists in the way that Hypertext Transfer Protocol (HTTP) connections are reused when NTLM authentication is used between front- end Exchange 2003 servers providing Outlook Web Access (OWA) and, OWA on Windows 2000 and Windows Server 2003, and when using back- end Exchange 2003 servers that are running Windows Server 2003. Users who access their mailboxes through an Exchange 2003 front- end server and OWA might get connected to another user's mailbox if that other mailbox is (1) hosted on the same back- end mailbox server and (2) if that mailbox has been recently accessed by its owner. Attackers seeking to exploit this vulnerability could not predict which mailbox they might become connected to. The vulnerability causes random and unreliable access to mailboxes and is specifically limited to mailboxes that have recently been accessed through OWA. This vulnerability is exposed if the Website that is running the Exchange Server 2003 programs on the Exchange back- end server has been configured not to negotiate Kerberos authentication, causing OWA to fall back to using NTLM authentication. The only known way that this vulnerability can be exposed is by a change in the default configuration of Internet Information Services 6.0 on the Exchange back- end server. Microsoft has assigned a severity rating of "Moderate" to this issue.

Category 24.4	TCP/IP & HTTP
2004-03-22	security vulnerability flaw hole patch fix exploit open source Apache Web server HTTP

DHS IAIP Daily;

March 19, eWEEK — Security holes uncovered in Apache.

Security researchers on Friday, March 19, uncovered a vulnerability in the open- source Apache Web server software that could easily enable a denial of services attack. The Apache problem is one of several reported in Version 2.0.48, and lets an attacker open a short- lived connection on a particular, rarely accessed listening socket. The software will block out all other connections until another connection comes in on the same socket. The Apache Software Foundation released update to its HTTP Server software that fixed the problem as well as several others:

http://www.apacheweek.com/redirect.cgi?link=http://www.apache.org/

Category 24.4 TCP/IP & HTTP

### 2004-04-20 Internet security flaw fix experters disrupt communications routers TCP/IP protocol

DHS IAIP Daily;

http://www.washingtonpost.com/wp- dyn/articles/A27890- 2004Apr 20.html

April 20, Washington Post — Experts race to fix serious Internet flaw.

Computer security experts in the U.S. and UK confirmed Tuesday, April 20, that a new method has been identified that could make it easy for hackers to disrupt Internet communications worldwide. The exploit, identified by Milwaukee security researcher Paul Watson, could give hackers the ability to crash Internet routers- - the complex machines that direct most of the world's Web traffic. Watson's method takes advantage of an inherent design flaw in transmission control protocol (TCP)- - the language that all computers use to communicate on the Internet- - that could place ordinary computers at greater risk of attack. Watson is slated to present his findings at a security conference in Canada later this week. Amit Yoran, director of the cybersecurity division for the Department of Homeland Security, said most of the world's major Internet service providers had already taken steps to prevent the attack. Additional information is availabe in "Technical Cyber Security Alert TA04- 111A: Vulnerabilities in TCP," available on the U.S. Computer Emergency Readiness Team Website:

http://www.us- cert.gov/cas/techalerts/TA04- 111A.html. The UK's National Infrastructure Security and Coordination Center has posted a vulnerability notice here:

http://www.uniras.gov.uk/vuls/2004/236929/index.htm

## Category24.4TCP/IP & HTTP2004-04-20TCP Transmission Control Protocol design flaw disrupt Internet router

NewsScan

SERIOUS FLAW IN TCP FOUND

Computer security experts in the U.S. and Britain have identified an inherent design flaw in the transmission control protocol (TCP) that could make it easy for hackers to disrupt Internet activities worldwide. Paul Watson, the security researcher who sounded the alarm over the flaw, warns it could be used to disable Internet routers -- the complex machines that direct most Internet traffic -- by tricking them into resetting themselves. Apparently, security experts have known for years about the basic vulnerability, but discounted its threat because attackers would have to successfully guess several specific sets of information in order to exploit it -- something that many thought would take several years using powerful computers. Watson appears to have discovered a shortcut that makes it possible to complete that task in just a few minutes. U.S. Homeland Security cybersecurity director Amit Yoran says despite the seriousness of the problem, most of the world's major Internet service providers have already quietly taken steps to protect themselves: "It's important to note that this is a significant discovery, but it's also important to provide a fair degree of assurance that the sky is not falling." (Washington Post 20 Apr 2004)

Category 24.4	TCP/IP & HTTP
2004-04-21	TCP injection vulnerability Border Gateway Protocol Initial Sequence Number DoS routers

http://searchsecurity.techtarget.com/originalContent/0,289142,sid14\_gci960715,00. html?track=NL-102&ad=480263

In April 2004, the technical press responded strongly to notices of some fundamental flaws in the TCP/IP suite. \* The "TCP Injection Vulnerability" could work with a problem in the Border Gateway Protocol to allow remote termination of network sessions, potentially leading to denial of service.

\* The "TCP/IP Initial Sequence Number Vulnerability" could permit data corruption, session hijacking and denial of service.<

Internet Security Systems (ISS) stated that "network infrastructure providers and enterprises' internal networks ...[are] the most vulnerable to potential denial-of-service/distributed denial-of-service attacks that can cause significant outages and downtime to users and customers."

Shawna McAlearney, writing for SearchSecurity.com, summarized recommendations as follows: "Experts recommend immediately applying patches issued by affected vendors. Workarounds include: ingress and egress filtering; prohibiting externally initiated inbound connections to non-authorized services and preventing machines providing public services from initiating outbound connections to the Internet; deploying and using cryptographically secure protocols, such as IPSec; and network isolation."

Category 24.4 TCP/IP & HTTP

2004-07-31 domain name service DNS vulnerability Defcon 12 presentation intellectual property theft

DHS IAIP Daily;

http://news.com.com/Internet%27s+%27white+pages%27+allow+dat a+attacks/2100- 1002\_3- 5291874.html?tag=nefd.hed

July 31, CNET News.com — Internet's 'white pages' allow data attacks.

The same technology that allows Web surfers to locate and connect to computers on the Internet can be used to create covert communications channels, bypass security measures and store distributed content, a security researcher said at the Defcon hacking conference in Las Vegas, NV, Saturday, July 31. The security hack essentially uses data transferred by domain name service (DNS) servers to hide additional information in the network communications. DNS servers act as the white pages of the Internet, invisibly transforming easy- to- remember domain names into the numerical network addresses used by computers. Moreover, corporate security measures, such as firewalls, tend to ignore DNS data because they assume it's harmless, said Dan Kaminsky, a security researcher for telecommunications firm Avaya said. That flaw in most companies' network security leaves a vulnerability that can be used by hackers to sneak intellectual property outside a company, communicate with a compromised server inside the company, or gain free access to many wireless and Internet services found in coffee houses and hotels, he said.

Category 24.4 TCP/IP & HTTP

2004-08-11 IBM Tivola vulnerability http response splitting input validation patch issued

DHS IAIP Daily; http://www.zone- h.org/advisories/read/id=5254

August 11, zone- h — IBM Tivoli Access Manager HTTP response splitting vulnerability.

A vulnerability has been discovered in IBM Tivoli Access Manager for e- business, which can be exploited by malicious people to conduct cross- site scripting attacks. The vulnerability is caused due to insufficient input validation and can be exploited to inject malicious characters into HTTP headers. This may allow execution of arbitrary HTML and script code in a user's browser session associated with an affected site. According to the vendor, successful exploitation may allow people to gain access and control over an affected system. A patch is available from the vendor.

Category 24.4 TCP/IP & HTTP

2004-10-07 Internet Protocol IP v6 security protocol adoption interest Internet

DHS IAIP Daily; http://www.gcn.com/vol1\_no1/daily- updates/27552- 1.html

October 07, Government Computer News — Market for IPv6 security is starting to grow.

Internet Protocol Version 6 (IPv6) is still in the early adoption phase, but commercial demand for tools to secure IPv6 networks is beginning to grow, according to one vendor. The Defense Department, which has committed to moving its networks to IPv6 by fiscal 2008, is the largest government customer for the security products. IPv6 provides improved security, increased IP address space and greater authentication capabilities to the Internet. Jim Bound, chairman of the North American IPv6 Task Force, said Japan now is the only country with a production IPv6 Internet backbone. Other networks, such as the Moonv6 test bed in the United States, are in pilot phases.

## 24.5 LAN OS

Category 24.5 LAN OS

### RSA Cfengine daemon vulnerability network administration tool fix patch issued

### DHS IAIP Daily;

2004-08-09

http://www.coresecurity.com/common/showdoc.php?idx=387&idxse ccion=10

August 09, Core Security Technologies — Cfengine RSA authentication heap corruption.

Cfengine, the configuration engine, is a very high level language for simplifying the task of administrating and configuring large numbers of workstations. Two vulnerabilities were found in cfservd, a daemon which acts as both a file server and a remote cfagent executor. This daemon authenticates requests from the network and processes them. If exploited, the first vulnerability allows an attacker to execute arbitrary code with those privileges of root. The second vulnerability allows an attacker to crash the server, denying service to further requests. Cfservd uses an IP based access control (AllowConnectionsFrom) which must be passed before the vulnerabilities can be exploited. The level of risk thus depends on how this access control is configured. These vulnerabilities are present in versions 2.0.0 to 2.1.7p1 of cfservd. Release 2.1.8 which fixes these vulnerabilities is available from http://www.cfengine.org.

Category 24.5 LAN OS

### 2004-12-06 Novell NetMail network messaging application protocol NMAP authentication failure

DHS IAIP Daily; http://www.securitytracker.com/alerts/2004/Dec/1012429.html

December 06, SecurityTracker — Novell NetMail default authentication credentials lets remote user access the mail store.

Novell reported that if the default Network Messaging Application Protocol (NMAP) authentication credentials have not been changed after installation, a remote user can connect to port 689 to gain access to the mail store. A remote user can also send unauthorized messages to other local or remote users. The default NMAP authentication credential is set automatically during installation but should be changed after installation using the nmapcred utility. As a solution, Novell indicates that you should use the NMAP Server Credential Generator (nmapcred) to set a unique NMAP authentication credential. Original advisory: http://support.novell.com/cgi- bin/search/searchtid.cgi?/2970 344.htm

# 24.6 WAP, WEP, Wi-Fi, Bluetooth, 802.11, WiMax

Category 24.6 WAP, WEP, Wi-Fi, Bluetooth, 802.11, WiMax

### 2004-01-08 wireless tracking technology licensed Motorola Steve Wozniak

NewsScan

MOTOROLA LICENSES WOZNIAK'S WIRELESS TRACKING TECHNOLOGY

Motorola is licensing technology developed by Apple co-founder Steve Wozniak's new venture, Wheels of Zeus. The wireless tracking system, dubbed "wOzNet," uses a wireless tag that links to GPS satellites and transmits location information via low-power radio signal. "Let's say you're a parent, you have four kids, and as soon as they hit the amusement park they run in four directions," says Motorola Broadband business development director Vince Izzo. "You could set the thing to let you know if any of them is more than 50 feet away from you." The technology could also enable a parent to monitor a child in the park without going along — the signal could be picked up by a cell phone company or local park operators and transmitted via the Internet to a base station in the parent's home. (AP/USA Today 8 Jan 2004)

Category 24.6	WAP, WEP, Wi-Fi, Bluetooth, 802.11, WiMax			
2004-01-26	wireless risks Wi-Fi security threat shared sensitive info	mation		
RISKS		23	16	
ANOTHER WIRELESS RISK				

Contributor Chris Meadows writes about an experience of his with wireless networking. When at Kinko's, needing print a credit card invoice urgently, Meadows scanned for an available printer on a wireless network. He found an open router called "linksys" which had a Lexmark printer connected to it. Meadows printed his CC invoice on this linksys printer. When he asked the Kinko's clerk where this printer was, the clerk responded, "[B]ut we don't have a wireless network...and we don't have any Lexmark printers either." Meadows had printed his invoice to a "stranger's printer." But Meadows assures us that the invoice contained no really sensitive information, and was closing that account anyway. Commenting on his experience, he says the risk with wireless networking, instead of "you never know who might be using your network," is, "you never know whose network you might be using."

Category 24.6	WAP, WEP, Wi-Fi, Bluetooth, 802.11, WiMax
2004-01-28	WAN security wireless internet wardriving

NewsBits; http://insight.zdnet.co.uk/0,39020415,39143769,00.htm

Category 24.6 WAP, WEP, Wi-Fi, Bluetooth, 802.11, WiMax

### 2004-02-03 NTIA Wi-Fi wireless broadband applications license

DHS IAIP Daily;

http://www.govtech.net/news/news.php?id=87078&e=1&u=/nm/20040203/tc\_n m/tech\_microsoft\_dc

February 03, Government Technology - NTIA seeks to expand spectrum available for high- speed Internet.

Last week, the National Telecommunications and Information Administration (NTIA) announced it was considering an expansion of the 3650- 3700 MHz band to unlicensed devices for wireless broadband applications such as Wi- Fi while protecting federal operations in those bands from interference or other adverse effects. NTIA has invited interested parties to file comments on technical requirements and interference- mitigation techniques necessary for compatible unlicensed device usage in those bands. "We want to make more spectrum available so that people who live in rural areas can have access to wireless broadband," said Acting Assistant Secretary of Commerce Michael D. Gallagher. "This continues our progress in facilitating the sharing of spectrum among government and commercial users." The filing says it appears that "very significant benefits" to the economy, businesses, consumers, and government agencies can be gained by allowing unlicensed devices to operate in other certain bands at higher power levels than currently permitted.

### Category 24.6 WAP, WEP, Wi-Fi, Bluetooth, 802.11, WiMax

2004-02-16 Bluetooth mobile wireless transponders policy portable laptop notebook PDA

http://searchmobilecomputing.techtarget.com/originalContent/0,289142,sid40\_gci 950572,00.html?track=NL-102

Gartner Group warned that Bluetooth-enabled devices pose a threat to data confidentiality due to security flaws in implementation. In particular, notebook computers and Internet enabled PDAs are at serious risk of compromise. Eric Panzo, News Editor of SearchMobileComputing.com, notes, "Gartner's recommendation comes after a week when two manufacturers disclosed that Bluetooth security vulnerabilities exist in nearly a dozen wireless handsets. On Wednesday [2004-02-11], Sony Ericsson revealed that several of its handsets, including the Sony Ericsson T610 and T68i and the Ericsson T39, T68 and R520, are vulnerable to attackers who could use Bluetooth to steal information stored on the devices. Earlier, Nokia had confirmed that a number of its handsets have a similar flaw. Affected handsets include the 6310, 6310i, 7650, 8910 and 8910i."

Category 24.6 WAP, WEP, Wi-Fi, Bluetooth, 802.11, WiMax

### 2004-02-18 Wi-Fi Internet connectivity spreading

NewsScan

WI-FI EVERYWHERE

Wi-Fi is in the air, and increasingly is being used for such household tasks as paying bills, searching for recipes from the kitchen and doing e-mail, and in the future it will be used to connect lamps, stereos, computers, and to integrate the Internet fully into daily life. Now, Wi-Fi is already being used in some consumer electronics, such as TVs, DVD players, stereos and other systems from Gateway, Microsoft, Samsung and others that make it possible to download a movie or song from the Internet and send it wirelessly to a home entertainment system. Still on the way: Wi-Fi systems to control your lights remotely, adjust your thermostat, check whether you left the iron on, and live your life as Mr. or Ms. Internet of the 21st century. (USA Today 18 Feb 2004)

Category 24.6	WAP, WEP, Wi-Fi, Bluetooth, 802.11, WiMax
---------------	---

### 2004-03-28 new WiFi wireless technology high speed networking Internet

NewsScan

FOUR NEW WIRELESS TECHNOLOGIES

Four new wireless technologies are now in the pipeline, and are expected to be ready for use by early 2005. The first is WiMax, which will have a reach up to 30 miles away and be competitive with cable and DSL for use by Internet service providers. The second is the 802.16e standard, an extension to WiMax that will allow connection to the Internet while a user is in a moving vehicle. The third is 802.11n, a high-bandwidth extension to the current Wi-Fi standard that would increase the speed of Wi-Fi connections by 10 to 20 times. And the fourth is Ultrawideband, which could be used for transmitting large amounts of data short distances. Jeff Harris of General Atomics explains Ultrawideband by offering this example: "We want to eliminate that cable that goes between devices. If you go and drop a few thousand dollars on a flat-panel television, we want you to be able to put it on the best wall in your house — not just the wall that's closest to the cable outlet." (USA Today 28 Mar 2004)

Category 24.6 WAP, WEP, Wi-Fi, Bluetooth, 802.11, WiMax 2004-03-31 **Department of Defense DoD WiFi issue policy IEEE 802.11b** 

NIPC/DHS

March 31, Government Computer News — DOD set to issue policy on WiFi use.

The Department of Defense (DoD) will soon issue a policy to guide the use of WiFi equipment, said Ronald Jost, director of wireless technology for the DoD. Jost spoke Wednesday, March 31, in Washington, D.C. at the National High Performance Computing Conference. The new policy will mandate that no information—either classified or unclassified—will be allowed to travel unencrypted across a wireless network. But DoD will encourage use of wireless networks, as they reduce the amount of time it takes to set up and tear down LANs. DoD currently has top- secret, local IEEE 802.11b networks running, Jost said. Offices can now procure military- grade secure equipment, so the remaining hurdles involve establishing policy, Jost said. The policy, DOD 8100.bb, is finished and awaiting sign- off, Jost said. DoD also will establish Websites instructing offices how to set up wireless networks for both classified and unclassified use. DoD is also developing a policy for the use of cellular phones. Jost said the department will establish relationships with selected commercial providers who will be able to provide military personnel with cellular voice and data connections. The process will involve companies certifying their equipment as secure. "All [cellular] data traffic will go through virtual private networks," Jost said.

Category 24.6 WAP, WEP, Wi-Fi, Bluetooth, 802.11, WiMax

2004-04-13 WiFi wireless network hacking SANS threat

NewsScan

WIRELESS HACKING

Pointing to a rise in wireless hacking, security expert Joshua Wright of the SANS Institute warns: "All the money you've spent to protect your corporate network is moot if someone hacks your laptop at a wireless access point." And Don LeBeau of security firm Aruba Wireless Networks says that at least one Silicon Valley company suspected it was the target of corporate espionage when it found an unauthorized device surrpetiously establishing a hot spot from a conference room. Shai Guday, group program manager for wireless at Microsoft, urges companies to take the wireless hacking threat seriously: "Wireless is happening. They can't bury their heads in the sand. Wireless is great, but security is more important." (USA Today 13 Apr 2004)

Category 24.6 WAP, WEP, Wi-Fi, Bluetooth, 802.11, WiMax

### 2004-05-03 wireless airlines air travel snail mail

DHS IAIP Daily;

http://www.dmnews.com/cgi- bin/artprevbot.cgi?article\_id=2734 5

May 03, DM News — Airlines use wireless tracking to comply with USPS contracts.

At least two airlines are working with a wireless company based in Redmond, WA, to track mail as it moves through their systems as part of their contracts with the U.S. Postal Service (USPS). The data is used by the postal service to verify whether an airline is adhering to on- time performance standards. Depending on the results, a carrier could lose, maintain, or gain postal business. As part of contracts awarded last year, carriers are required by the USPS to scan mail at the time it is received, when the carrier loads the mail onto a flight, during transfers to connecting flights, and upon delivery to the postal service. The change to the contract process came about in part from Federal Aviation Administration security restrictions put in place after September 11. Air Transport Association statistics indicate that carriers last year flew 1.3 billion mail revenue ton miles, which is one ton of mail payload transported one mile.

Category 24.6 WAP, WEP, Wi-Fi, Bluetooth, 802.11, WiMax

### 2004-05-05 Wi-Fi Wireless security WPA WEP 802.11i

DHS IAIP Daily; http://www.pcworld.com/news/article/0,aid,115999,00.asp

May 05, IDG News Service — Wi- Fi security improves.

Two key improvements for the security and performance quality of Wi- Fi devices are scheduled to reach wireless network users this year as businesses and consumers continue to adopt wireless technology in greater numbers. The Wi- Fi Alliance will certify products for the new 802.11i and 802.11e standards by September, says Frank Hanzlik, managing director of the Wi- Fi Alliance. The 802.11i standard is the complete version of the preliminary security standard WPA (Wi- Fi Protected Access) introduced last year, while 802.11e is a new standard that will improve the quality of wireless networks that transmit voice and video. Security has been one of the biggest obstacles to the growth of wireless networking. Last year, WPA replaced the flawed Wired Equivalent Privacy (WEP) protocol to shore up wireless security before the full 802.11i standard could be ratified. WPA uses a dynamic encryption key as opposed to the static key used by WEP, and it also improves the user authentication process. The 802.11i standard adds Advanced Encryption Standard (AES) technology, a stronger level of security than used in WPA.

Category24.6WAP, WEP, Wi-Fi, Bluetooth, 802.11, WiMax2004-05-10wireless Wi-Fi security Trusted Computing Group TSG

DHS IAIP Daily; http://www.eweek.com/article2/0,1759,1590243,00.asp

May 10, eWEEK — Spec in works to secure wireless networks.

The Trusted Computing Group (TSG) said Monday, May 10, that it is working on a specification to ensure that wireless clients connecting to a network won't serve as a back door to worms and crackers. The specification will be finalized later this year. Although a client or customer connecting to an enterprise network may not overtly be seeking to do harm, the laptop may in fact hide an unpatched system that could serve as an unexpected back door into an otherwise secure system. Likewise, a network administrator cannot be sure whether a laptop hides a worm that might otherwise have been blocked by a wired firewall. When completed, the specification will serve as a means by which network security and network infrastructure vendors can ensure a level of compliance with the best practices of network security, executives said. The specification will specify a level of trust for network endpoints, characterized by the version number of specific applications; whether those applications have been patched; and whether those OSes and applications are free from viruses, as defined by the revision numbers of the signature libraries used within antivirus applications. If a client fails to meet those specifications, the Trusted Network Connect specification will define a process by which the client is quarantined until the appropriate patches and anti- virus tools have been applied.

Category 24.6 WAP, WEP, Wi-Fi, Bluetooth, 802.11, WiMax

### 2004-05-11 Bluetooth wireless security bluesnarfing

DHS IAIP Daily;

http://www.computerworld.com/printthis/2004/0,4814,93066,00.html

May 11, Computerworld — Bluetooth group downplays security risks.

The Bluetooth Special Interest Group (SIG) is dismissing security fears about the technology. Mike McCamon of Bluetooth SIG said Monday, May 10, that Bluetooth device shipments have now hit one million per week and that any security problems with the wireless technology security problems are limited to a handful of phones manufactured by Nokia Corp. and Sony Ericsson Mobile Communications AB. Those phones, which include Sony Ericsson's R520m and T68i phones and Nokia's 6310, 6310i, 8910 and 8910i phones, are susceptible to a hacking technique known as "bluesnarfing," according to Nick Hunn, a Bluetooth security expert in London. Flaws in these phones can allow hackers to access data such as information stored in address books or calendars, he said. Both Nokia and Sony Ericsson are developing patches for the older phones, while newer models won't be vulnerable to a bluesnarfing attack, Hunn said. Nokia said that it views any security threat from bluesnarfing as minimal and that the technique can be easily prevented by setting Bluetooth on the phones to a "hidden" mode. That makes intrusion more difficult, "since the hacker will have to know or guess the Bluetooth address before establishing a connection," said Nokia.

Category 24.6 WAP, WEP, Wi-Fi, Bluetooth, 802.11, WiMax

### 2004-05-13 CERT AusCERT vulnerability wireless 802.11

DHS IAIP Daily; http://www.auscert.org.au/render.html?it=4091 Source: http://www.kb.cert.org/vuls/id/106678

May 13, US- CERT — Vulnerability Note VU#106678: IEEE 802.11 wireless network protocol DSSS CCA algorithm vulnerable to denial of service.

The Clear Channel Assessment (CCA) algorithm used in conjunction with Direct Sequence Spread Spectrum (DSSS) transmission is vulnerable to an attack in which a specially crafted RF signal will cause the algorithm to conclude that the channel is busy, so that no device in range of the signal will transmit data. The attacker must be actively transmitting a signal and within range to affect wireless devices. AusCERT notes that devices that use 802.11 and DSSS transmission encoding are affected. An unauthenticated, remote attacker can cause any vulnerable device within range to stop transmitting, causing a denial of service. A complete solution is not available for 802.11 DSSS devices. This vulnerability and potential workarounds are available in AusCERT Advisory AA- 2004.02: http://www.auscert.org.au/render.html?it=4091

Category 24.6 WAP, WEP, Wi-Fi, Bluetooth, 802.11, WiMax

2004-05-16 w-fi flaw Queensland University Australia 802.11 exploit

NewsScan

RESEARCHERS FIND WIFI FLAW

Researchers at Queensland University of Technology in Australia have discovered an easily-exploited vulnerability that can be used to take down most 802.11 wireless networks. The flaw operates at lower network layers than most previously-discovered security flaws in 802.11 networking, and affects any network operating at the 2.4GHz frequency — which is the sole frequency used by the most popular wireless protocol, 802.11b. (The Australian 13 May 2004) rec'd from John Lamp, Deakin U.

Category 24.6 WAP, WEP, Wi-Fi, Bluetooth, 802.11, WiMax

2004-05-17 Wi-Fi transportation airlines broadband

DHS IAIP Daily; http://www.newscientist.com/news/news.jsp?id=ns99995001

May 17, New Scientist - Hi- flying Wi- Fi debuts on transatlantic flight.

Passengers flying on a Lufthansa flight from Munich to Los Angeles on Monday, May 17, became the first to experience in- flight Wi- Fi - a broadband wireless internet connection. The satellite- based system enables passengers to surf the web and send emails from their own Wi- Fi- enabled laptop or handheld computers instead of using the more limited services some airlines offer through their seatback displays. The system, called FlyNet, has already been installed on five of Lufthansa's fleet, with plans to extend this to all 80 of the German airline's long- haul planes by the end of 2006. The cost to passengers is \$10 for half an hour, or a flat rate of \$30 for the entire flight. This is far cheaper that the \$16 per email charged by some companies via seatback equipment. Internet traffic to and from the aircraft is handled via geostationary communications satellites orbiting the Earth at 36,000 kilometres.

Category 24.6 WAP, WEP, Wi-Fi, Bluetooth, 802.11, WiMax

### 2004-05-25 Wireless Wi-Fi WLAN flaw vulnerability defense

DHS IAIP Daily; http://www.computerworld.com/securitytopics/security/holes/s tory/0,10801,93343,00.html?SKC=security- 93343

May 25, ComputerWorld — IT managers ready defenses against flaw in wireless LANs.

Information technology managers last week said a denial- of- service vulnerability that affects some Wi- Fi wireless LANs (WLANs) could force companies to develop new skills and rethink the way their networks are set up. But, they added, it should be relatively easy to defend WLANs against attacks seeking to exploit the flaw. Companies that operate multiple access points on their WLANs could also switch network traffic to other access points if one or more were attacked, although doing so would require radio frequency management skills and tools. The flaw was discovered by a team of graduate students at Queensland University of Technology in Brisbane, Australia. Mark Looi, a professor there, suggested that one defense against attacks would be to replace all 802.11b access points with 802.11a technology, which uses a different form of modulation than DSSS.

Category 24.6 WAP, WEP, Wi-Fi, Bluetooth, 802.11, WiMax

2004-06-09 Wi-Fi spread NBA stadium access

NewsScan

WI-FI EVERYWHERE?

The head of arena operations for the Charlotte Bobcats, an NBA expansion team, is including Wi-Fi wireless communications in the design of the team's new \$265 million arena. He says, "Some people will think this is the geeky thing, the nerdy thing. But they were probably saying that 10 years ago when other people were going to Web sites and using e-mail." Other professional sports teams are making the same moves, and Giants chief information officer Bill Schlough says: "It's like walking into Starbucks. Except our Wi-Fi is free." Using Wi-Fi, fans will be able to access content

such as historical videos, trivia games and real-time statistics from the Internet or through customized material available only in the stadium. Schlough says: "There's a lot of purist fans who scoff at anybody bringing laptops to games. I've been heckled when I go in the stands. But then

they'll end up wanting to look over your shoulder." His only fear: "The real problem is business people coming and doing their office e-mails at the game." (USA Today 9 Jun 2004)

## Category24.6WAP, WEP, Wi-Fi, Bluetooth, 802.11, WiMax2004-06-11broadband WiFi spectrum reconfiguration Federal Communications Commission<br/>FCC

NewsScan

FCC PAVES THE WAY FOR SPECTRUM RECONFIGURATION

The Federal Communications Commission approved a plan to reconfigure a chunk of valuable airwave spectrum in an effort to boost wireless broadband use. The current configuration places spectrum intended for educational-video use adjacent to spectrum earmarked for commercial uses -- a situation that requires the agency to impose rigid rules on commercial users to avoid interference. The FCC also decided to maintain its policy of allowing educators to lease spectrum to companies such as Nextel and Sprint, but ruled against allowing the widespread sale of educational

licenses. Currently, schools can license 120 megahertz of the 194 MHz band, and educators are permitted to lease as much as 95% of their airwaves to commercial users and spend the proceeds for educational purposes. Critics had charged that some educators had not made good use of their licenses, but most educators opposed outright sale of the licenses, comparing the idea to the sale of national parks. (Wall Street Journal 11 Jun 2004)

Category 24.6 WAP, WEP, Wi-Fi, Bluetooth, 802.11, WiMax

### 2004-08-06 computer science research team Wi-Fi security study weakness RSA RPI

DHS IAIP Daily; http://www.stevensnewsservice.com/pr/pr460.htm

August 06, Stevens News Service — CompSci team spots weaknesses in Wi- Fi security.

A research team led by Dr. Susanne Wetzel, an Assistant Professor of Computer Science at Stevens Institute of Technology, has produced a study of the weaknesses of Wi- Fi networks. Wetzel's team has discovered "stealth attack" methods of disrupting and draining power from individual nodes within an "ad hoc" wireless network- - i.e., a network that one "connects to" as a visitor as one moves physically with one's mobile computer from location to location, without a dedicated access point. While still rare, ad hoc modes are the underpinning for many of the advanced data networking schemes now being proposed. "Most of today's communication infrastructure is based on trustworthy collaboration among information routers," says Wetzel. "However, given the increased economic reliance on a working communication infrastructure, this has become a potential target for terrorists and other criminals." Wetzel worked with researchers from Rensselaer Polytechnic Institute and RSA Labs, as well as Stevens' own Wireless Network Security Center (WiNSeC).

Category 24.6 WAP, WEP, Wi-Fi, Bluetooth, 802.11, WiMax

### 2004-08-12 Widcomm Bluetooth virus vulnerability PDA PC

DHS IAIP Daily; http://www.esecurityplanet.com/alerts/article.php/3394181

August 12, eSecurity Planet — Widcomm Bluetooth a virus risk.

A security research firm has discovered a serious vulnerability in Widcomm's widely deployed Bluetooth Connectivity Software that could lead to wireless delivery of malicious worms and viruses. According to an advisory from British security firm Pentest, an unauthenticated remote attacker could exploit the flaw to submit malformed service requests via Bluetooth, which would trigger a buffer overflow. Buffer overflows are commonly used by malicious hackers to execute arbitrary code on vulnerable systems. In theory, security experts say this could pave the way for the creation of a wireless worm that spreads between PCs or PDAs using Bluetooth over the air. "Worms like this could spread very fast, especially in an environment like a seminar or a conference," said Jarno Niemela, a virus tracker at F- Secure.

## Category 24.6 WAP, WEP, Wi-Fi, Bluetooth, 802.11, WiMax 2004-09-02 New York City NYC Republican National Convention RNC 2004 elections wireless security challenge Wi-Fi war driving unencrypted hot spots access points discovery

DHS IAIP Daily;

http://www.computerworld.com/mobiletopics/mobile/story/0,108 01,95641,00.html

September 02, Computerworld — Manhattan presents wireless security challenge for RNC.

IT security researchers have uncovered a significant number of unencrypted wireless devices in close proximity to the Republican National Convention (RNC) at New York's Madison Square Garden. During a two- hour "war drive" around the site of the RNC as well as Manhattan's financial district, security researchers from Newbury Networks Inc. discovered more than 7,000 wireless devices, 1,123 of which were located within blocks of the convention. More important, 67% of those devices were access points that did not have encryption protection. The findings underscore that the huge numbers of open, unsecured wireless networks represent a serious threat to the city's hard- wired infrastructure, said Newbury CEO Michael Maggio. "A wireless- enabled notebook computer powered up inside Madison Square Garden by a conventioneer or media representative could automatically associate with wireless networks outside of the building," said Maggio, noting that such a security gap could allow an attacker to "hop onto" the wired network inside the facility.

Category 24.6 WAP, WEP, Wi-Fi, Bluetooth, 802.11, WiMax

2004-09-02 Philidelphia free wireless Wi-Fi access Internet hot spot largest world

NewsScan

SOFTWARE AND THE CITY

Philadelphia officials are considering a plan to turn the whole city into the world's largest wireless Internet hot spot, placing thousands of small Wi-Fi transmitters around the city. Philadelphia chief information officer Dianah Neff says, "If you're out on your front porch with a laptop, you could dial in, register at no charge, and be able to access a high speed connection. It's a technology whose time is here." The Philadelphia service wouldn't be the first city to do this, only the largest so far. The Minneapolis suburb of Chaska began offering citywide wireless Internet access this year for \$16 a month (to an area of about 13 square miles), and Cleveland has positioned 4,000 wireless transmitters in several areas, offering free Wi-Fi Internet access for anyone who passes through those

areas. Neff estimates it would cost Philadelphia \$1.5 million a year to maintain the system it's considering. (AP 2 Sep 2004)

Category 24.6 WAP, WEP, Wi-Fi, Bluetooth, 802.11, WiMax

### 2004-10-26 WiMax 802.16 Intel Craig McCaw

NewsScan; http://www.nytimes.com/2004/10/26/technology/26intel.html

INTEL TEAMS WITH MCCAW STARTUP ON WIMAX NETWORKS

Intel is collaborating with Clearwire, a startup founded by cellular mogul Craig McCaw, to jumpstart WiMax technology by creating a series of new chips designed to support the WiMax standard. WiMax is intended to extend the limited reach of WiFi wireless networks by permitting a single transceiver to connect hundreds or thousands of customers to the Internet over distances of many miles. Clearwire recently began offering wireless Internet service in Jacksonville, Fla., for \$25 a month and plans to be available in as many as 20 U.S. markets by next year. It's also deploying the service in Canada and Mexico, as well as in developing countries like Bangladesh. "We are tempered by the fact that everyone who has tried this has failed," says McCaw, "but w'ere crossing the river on the backs of pioneers." (New York Times 26 Oct 2004)

Category 24.6 WAP, WEP, Wi-Fi, Bluetooth, 802.11, WiMax

### 2004-11-17 WiFi cellphones dual-network NTT DoCoMo 3G

NewsScan; http://apnews.excite.com/article/20041118/D86E0F280.html

NTT OFFERS DUAL-NETWORK CELL PHONE NTT

DoCoMo is offering customers a cell phone that can make Internet calls via WiFi networks in addition to using the standard wireless networks. The dual-network N900iL phone uses 3G technology to deliver higher speed data transmissions. Nokia, the world's largest handset maker, says it will introduce a dual-network cell phone next year. (AP 17 Nov 2004)

### Category24.6WAP, WEP, Wi-Fi, Bluetooth, 802.11, WiMax2004-11-23municipal WiFi MAN Verizon Pennsylvania legislation

NewsScan; http://online.wsj.com/article/0

TELCOS THREATENED BY MUNICIPAL WIFI

Dozens of municipalities around the country are installing WiFi networks in order to provide citizens with low- or no-cost wireless Internet access -- a phenomenon that has raised the ire of large telephone and cable companies, who see their lucrative broadband businesses eroding. In response, telcos and cable companies are pushing states to pass legislation that could make such municipal networks illegal. Last week, after intensive lobbying by Verizon, the Pennsylvania General Assembly passed a bill with a deeply buried provision that would make it illegal for any "political subdivision" to provide to the public "for any compensation any telecommunications services, including advanced and broadband services within the service territory of a local exchange telecommunications company operating under a network-modernization plan." Verizon is the local exchange operator for most of Pennsylvania and is planning a major fiber-optic cable rollout. Similar bills have passed in Utah, Louisiana and Florida. Critics say the telco giants' clout is stifling broadband expansion in the U.S., but the telcos argue it's unfair for them to have to compete against local governments, which have easy access to capital and pay no taxes. (Wall Street Journal 23 Nov 2004)

Category 24.6 WAP, WEP, Wi-Fi, Bluetooth, 802.11, WiMax

### 2004-11-29 WiMax 802.16 TowerStream New York

NewsScan; http://www.nytimes.com/2004/11/29/technology/29max.html

WIMAX PROSPECTS LOOKING UP

Upstart TowerStream is offering a new take on wireless broadband, delivering highspeed connections to business customers through antennas perched atop highrises in urban areas. The service, dubbed WiMax (worldwide interoperability for microwave access), uses fixed antennas to send and receive signals across entire metropolitan areas. The radio signals and antennas are unaffected by bad weather and provide a cheaper alternative to data cables buried below streets that are vulnerable to accidental severing by construction crews. Although other companies are getting into the WiMax business, TowerStream is currently the market leader, with a lock on prime locations like the top of the Empire State Building and the MetLife Building in New York City. "The real estate is the hard part of the business," says TowerStream COO Jeff Thompson. "When you tell people you can reach 10,000 clients, they don't believe you." It took him more than two years to negotiate those leases, but Thompson's optimism is warranted, say many analysts. The high-speed wireless Internet market is worth about \$400 million globally and could quadruple in the next few years, according to the WiMax Forum, a group of WiMax equipment makers and providers. (New York Times 29 Nov 2004)

Category 24.6 WAP, WEP, Wi-Fi, Bluetooth, 802.11, WiMax

### 2004-11-30 wireless MAN municipal Philadelphia Verizon

NewsScan; http://www.siliconvalley.com/mld/siliconvalley/10305668.htm

WIRELESS IN PHILADELPHIA

Verizon has struck a deal with the city of Philadelphia to provide wireless Internet access as a municipal service. A spokeswoman for Philadelphia Mayor John F. Street says the two parties "reached an understanding that protects our interests and allows us to move forward with the Wireless Philadelphia initiative." Under the Pennsylvania legislation, any political subdivision would have to get the permission of the local telephone company to provide a telecommunications service for a fee, including broadband Internet, and if the company rejects the plan it would have to offer a similar service within 14 months. (San Jose Mercury News 30 Nov 2004)

### Category 24.6 WAP, WEP, Wi-Fi, Bluetooth, 802.11, WiMax

### 2004-12-15 wireless FCC airplanes Internet access

NewsScan; http://www.latimes.com/technology/ats-ap\_technology10dec15

WIRELESS ACCESS ON JETS?

The Federal Communications Commission (FCC) is considering a plan that would allow air travelers wireless high-speed Internet access. David Stempler, president of the Air Travelers Association, says the changes under consideration would "make business travelers more efficient and while away the time for a lot of other passengers. This is all the wave of the future here." (AP/Los Angeles Times 15 Dec 2004)

## 24.7 SWDR (Software-defined radio)

Category 24.7 SWDR (Software-defined radio)

### 2004-11-08 **P2P peer-to-peer Internet radio music sharing copyright**

NewsScan; http://news.com.com/Music+sharing+thats+free+and+legal/2100-1027\_3-5441036.html

P2P RADIO IS LATEST TWIST IN MUSIC SHARING

Now there's a new way to share music that's free and perfectly legal -- the trick involves marrying peer-to-peer technology with Internet radio. Pioneers in the field include Apple, Virgin Digital, and startups Mercora and Live 365, which offer tools that automatically stream users' private playlists over the Web while in some cases storing them in a searchable database for later retrieval. Mercora operates a Web-based network of about 8,000 "broadcasters" who serve up their playlists to somewhere between 175,000 and 200,000 listeners worldwide. "We're doing for music what Google did for the Web," says Mercora CEO Srivats Sampath. The company reasons that by using an Internet broadcast network model, it can take advantage of lower copyright fees, which are set by the U.S. Copyright Office rather than the record labels. As a result, Mercora can afford to pay the fees on behalf of broadcasters and offset the costs through advertising sales. "The big nut we had to crack is how to do this legally," says Sampath. "The law says you can broadcast as long as you pay. Fine, we will pay you." And if listeners happen to download a song? Technically, if the legally broadcast song is for personal use only, that's okay. "It's like a tape recorder," says Sampath. However, the downloader runs into legal trouble only when she tries to sell a track or transfer it to another person. (CNet News.com 8 Nov 2004)

## 24.8 MAC OS

Category 24.8 MAC OS

2004-03-02

### vulnerability hole flaw patch fix file sharing Mac OS X

DHS IAIP Daily; http://www.eweek.com/article2/0,1759,1540556,00.asp

February 27, eWEEK — File sharing vulnerability discovered in Mac OS X.

A security issue that could result in stolen passwords and data on Friday, February 27, was revealed for Apple Computer Inc.'s Apple Filing Protocol (AFP), a component of Mac OS X 10.3.2. In a posting to the SecurityFocus BUGTRAQ list, Chris Adams, a system administrator, noted that while users could request secure connections, the system will not issue any alert or indication if an SSH connection is unavailable and then defaults to a non- secure connection. The only indication was a negative one- - users must be aware that an alert "Opening Secure Connection" did not appear. This could result in users sending unencrypted passwords over an insecure connection. Adams said that any such activity would only come as the result of an active attack. "OS X does warn you before using unencrypted passwords and AFP does prevent passive password collection by encrypting the log- in process to protect the password on its way to the server. This problem allows you to trick it into sending the unencrypted password to you instead of the intended server," he said. Though his BUGTRAQ warning provided workarounds, such as manually configuring a SSH tunnel or using SFTP instead, Adams suggested that SSH should be enabled by default for both client and server and the user interface modified to clearly warn when the system is unable to establish an SSH tunnel. Additional information is available on the SecruityFocus Website: http://www.securityfocus.com/bid/9763/discussion/

Category 24.8 MAC OS

### 2004-05-04 Apple Mac OS X vulnerability patch issued

DHS IAIP Daily; http://www.esecurityplanet.com/prodser/article.php/3349191

May 04, eSecurityPlanet — Apple issues patch for Mac OS X.

Apple Computer has rolled out a major security update to plug several vulnerabilities in its flagship Mac OS X server and client versions. The patch, which is being described as "highly critical," addresses security issues with the AFP Server, CoreFoundation and IPSec and also integrates a previously issued patch which contained bugs, Apple said. The latest flaws, discovered by researchers at @Stake, could lead to system hijack, security bypass, manipulation of data, privilege escalation, denial- of- service attacks and system access. The most serious flaw was found with AppleFileServer and can be exploited to compromise a vulnerable system. The vulnerability is caused due to a boundary error within the password handling and could allow attackers to cause a buffer overflow by passing an AFP "LoginExt" packet with a string in the "PathName" field. Apple also confirmed the existence of an unspecified vulnerability. Another flaw in RAdmin when handling large requests was also pinpointed. Secunia warned that this issue could potentially lead to system compromise problems. Security update information: http://docs.info.apple.com/article.html?artnum=61798

### Category 24.8 MAC OS

### 2004-05-17 vulnerability MAC OS X security issue critical update issued

DHS IAIP Daily;

http://www.techworld.com/security/news/index.cfm?newsid=1574

May 17, Techworld — Mac OS X hit with another serious security issue.

A "highly critical" hole has been found in Apple's Mac OS X operating system, which will allow remote system access by getting someone to visit a malicious Website. Lixlpixel has reported a vulnerability dealing with how basic Internet elements are addressed in the OS' help facility that allow arbitrary local scripts to be executed on a user's machine. It is also possible to place files in a known location on a system by asking users to download a ".dmg" disk image file. A default browser option in Internet Explorer and Safari will mean a single user click is enough to drive the whole process. The combination of the two holes, tested and confirmed by security experts Secunia, can therefore allow system access to be achieved "very simply" according to Secunia CTO Thomas Kristensen. The holes affect Safari 1.x and Explorer 5.x. The solution is to change browser options and rename the help URI handler. More details are 11 available on Secunia's Website: http://secunia.com/advisories/11622

Category24.8MAC OS2004-05-21Apple OS X Mac vulnerabilities update issued

DHS IAIP Daily; http://www.reuters.com/newsArticle.jhtml?type=technologyNews &storyID=5224718

May 21, Reuters — Apple says OS X vulnerable to security breach.

Apple Computer Inc. said on Friday, May 21, a security hole in its software leaves users' computers vulnerable to attack. Apple, warning of a rare security hole in the company's OS X operating system for the second time this month, said in a release that a "theoretical vulnerability" in an application used to get help while browsing the Web could expose users to a malicious software code. The specific nature of the security hole, such as whether it makes the computer vulnerable to outsiders or allows virus- like code to enter the operating system, was not made clear. Apple urged users to go to its Website to download a free software update: http://www.apple.com/support/downloads/

Category 24.8 MAC OS

### Apple OS X Mac vulnerabilities run file IM e-mail virus

DHS IAIP Daily;

2004-05-25

http://news.com/Mac+OS+fix+fails+to+plug+security+hole/2 100- 1002\_3- 5220285.html

May 25, CNET News.com — Mac OS fix fails to plug security hole.

A security hole still threatens Mac OS X users after a patch issued by Apple Computer last week failed to fix the underlying problem, security experts say. The security issue could allow an attacker to transfer and then run a malicious program on a Mac, if the Mac's user can be enticed to go to a fake Web page on which the program has been placed. Two other software companies have confirmed the issue. Security information company Secunia raised its rating of the potential risk to "extremely critical" after determining that the vulnerability is more widespread than Apple apparently first thought. The vulnerability actually involves two flaws. One allows a website to place a file on the Mac's hard drive when a user clicks on a uniform resource locator, or URL, specifically designed to bypass Mac OS X's security. The other gives an attacker the ability to run a file on another user's computer, provided the location of the file is known. Used together, the flaws constitute a major security hole that could result in a potential instant- messaging or e- mail virus.

Category 24.8 MAC OS

### 2004-08-10 Apple Mac OSX 10.3.5 vulnerability PNG phishing attack

DHS IAIP Daily; http://www.esecurityplanet.com/patches/article.php/3392971

August 10, eSecurity Planet — Apple plugs OS X vulnerabilities.

Apple Computer has rolled out a major security update for its Mac OS X Panther client platform. The patch addresses security flaws that put users at risk of sensitive data leakage, Denial of Service attacks and system access. The Mac OS X 10.3.5 update corrects multiple vulnerabilities in libpng that can be exploited by malicious hackers to compromise a user's system. The U.S. Computer Emergency Readiness Team (US- CERT) has previously issued a warning that bugs in libpng, the reference library that supports the Portable Network Graphics (PNG) image format, could allow a remote attacker to commandeer a vulnerable machine. Also patched are specific vulnerabilities in Apple's Safari Web browser. The upgrade plugs a hole that could open the door to phishing attacks and addresses a flaw that could be used by a malicious Website to steal sensitive information from forms. The original advisory is available here: http://docs.info.apple.com/article.html?artnum=25631

Category 24.8 MAC OS

### 2004-08-16 Apple Safari Web browser vulnerability Mac OS X HTTP GET POST URL

DHS IAIP Daily; http://www.kb.cert.org/vuls/id/128414

August 16, US- CERT — Vulnerability Note VU#128414: Apple Safari fails to properly handle form data in HTTP redirects.

Apple Safari is a web browser available for the Mac OS X operating system. A vulnerability exists in the way Safari handles web form data. When a web form is submitted to a server using the POST method and the server returns an HTTP redirect to a GET method URL, Safari may re- POST that data to the GET method URL. It has been reported that this condition occurs when the forward/backward buttons are used. As a result, a user's form data could be disclosed to a remote server. Apple has released a patch to address this vulnerability: http://docs.info.apple.com/article.html?artnum=61798

## Category 24.8 MAC OS 2004-09-07 Apple Mac OSX operating system flaws vulnerabilities fixes patch Kerberos authentication Jaguar Safari browser

DHS IAIP Daily;

http://news.com.com/Apple+fixes+15+flaws+in+Mac+OS+X/2100- 10 02\_3- 5350010.html?tag=nefd.top

September 07, CNET News.com — Apple fixes 15 flaws in Mac OS X.

Apple Computer released an update to its Mac OS X operating system on Tuesday, September 7, to fix 15 security issues in the software. Many of the problems are flaws in the operating system's underlying open- source software, including a critical flaw in the Kerberos authentication system- - software that can act as a gatekeeper for computer networks. The patch is available for Mac OS X 10.3.5 and Mac OS X 10.3.4, and also fixes issues in Mac OS X 10.2, known as "Jaguar." The patch, available through automatic updates or from the company's website, fixes software flaws that could enable an attacker to crash or freeze the Apache 2 Web server, run software by utilizing Apple's Safari Web browser or expose the password store used by the network. Apple's advisory, with details of the update, is available at: http://www.apple.com/support/

Category 24.8 MAC OS

### 2004-10-28 Apple Remote Desktop privilege escalation vulnerability update issued

DHS IAIP Daily; http://secunia.com/advisories/11711/

October 28, Secunia — Apple Remote Desktop privilege escalation vulnerability.

A vulnerability has been reported in Apple Remote Desktop, which can be exploited by malicious users to gain root access on a vulnerable system The problem is that a user under certain circumstances during the login process is able to launch applications behind the login window with root privileges. Update to version 2.1 or apply Security Update 2004- 10- 27 for version 1.x available at: http://www.apple.com/support/downloads

Category 24.8 MAC OS

### 2004-11-03 National Security Agency NSA Mac OSX guidance

DHS IAIP Daily; http://www.gcn.com/vol1\_no1/daily- updates/27799- 1.html

November 03, Government Computer News — NSA gives security guidance for Mac OS X.

The National Security Agency (NSA) has posted a 109- page document on its Website

(http://www.nsa.gov/snac/os/applemac/osx\_client\_final\_v.1.pd f) telling agencies how to securely install and use Apple Computer Inc.'s Mac OS X Version 10.3.x operating system, code- named Panther. NSA notes that the document is a security guide and "not meant to replace well- structured policy or sound judgment." It warns administrators to test only in a non- production environment as similar as possible to the architecture where the OS will be deployed.

Category 24.8 MAC OS

### 2004-12-10 Adobe Version Cue Mac OSX privilege escalation vulnerability no update issued

DHS IAIP Daily; http://secunia.com/advisories/13399/

December 10, Secunia — Adobe Version Cue privilege escalation vulnerability.

A vulnerability in Adobe Version Cue is caused due to an error in the suid root scripts "startserver.sh" and "stopserver.sh". The current directory is not checked properly before executing scripts without an absolute path and can be exploited to gain root privileges by planting a malicious script named "productname.sh" in the current directory. The vulnerability has been reported on Mac OS X 10.3.6. Other versions may also be affected. No vendor solution is currently available.

## Category 24.8 MAC OS 2004-12-22 Apple Tiger suit data leakage BitTorrent intellectual property non-disclosure agreement NDA

NewsScan; http://news.bbc.co.uk/1/hi/technology/4117465.stm

APPLE SUES 'TIGER' TESTERS OVER LEAKS

Apple has sued three members of the Apple Developer Connection for releasing preview versions of its latest Mac OSX, codenamed Tiger, onto file-sharing sites. "Members of Apple Development Connection receive advance copies of Apple software under strict confidentiality agreements, which we take very seriously to protect our intellectual property," said Apple in a statement. The Apple Development Connection is a group of software programmers who have access to text versions of Apple software in order to tweak their own applications to work with Apple systems. The Tiger software was apparently leaked onto sites that use BitTorrent technology, which does not actually host the files being shared, but rather hosts a link that points users toward others who have the file sought. Last week, the Motion Picture Association of America launched a legal campaign against such sites, noting that they've been used for illegal sharing of movie files. (BBC News 22 Dec 2004)

## 24.9 Peer-to-peer networking

Category 24.9 Peer-to-peer networking

### 2004-01-22 virus threat peer-to-peer network P2P file music sharing

NIPC/DHS; http://news.bbc.co.uk/1/hi/technology/3409187.stm

January 20, BBC News - Viruses turn to peer-to-peer nets.

Virus writers are setting up peer-to-peer networks to help their malicious creations spread. The networks are being used to control thousands of innocent PCs that some virus programs have infected. The tactic is being used because peer-to-peer networks are hard to disrupt, making viruses using this technique hard to stop spreading. One of the first viruses to set up a peer-to-peer network to help it spread was the Slapper worm that was aimed at the Linux operating system. A Windows virus called Sinit appeared in late 2003 that turned every machine infected by the malicious program into a member of a peer-to-peer network. It was expected that Sinit's creator would issue commands to infected computers via this network. In the past some creators of Trojan programs, that open up a backdoor into an infected PC, have used net chat channels as a way to issue commands. Often thousands of computers were enrolled in these remote controlled networks that have been dubbed "bot nets." Finding and shutting down the chat channels would effectively cut a virus writer off from his network of slave machines. But shutting down a distributed network would be much more difficult because no one machine is in charge. It also is much more difficult to trace where commands were being inserted and find the network's controller.

 Category
 24.9
 Peer-to-peer networking

 2004-02-02
 peer-to-peer P2P music file sharing intellectual property rights lawsuit Grokster Morpheus

NewsScan

P2P CASE HEADS BACK TO COURT

A federal appeals court in California will review a lower court ruling made last spring that held distributing P2P software tools such as Grokster and Morpheus was legal and absolved the parent companies of responsibility for copyright infringement occurring on those networks. That ruling was a surprise setback for the entertainment industry, which had prevailed in previous efforts to shut down Napster and other file-swapping sites. In his decision last April, Judge Stephen Wilson wrote: "Defendants distribute and support software, the users of which can and do choose to employ it for both lawful and unlawful ends. Grokster and Streamcast are not significantly different from companies that sell home video recorders or copy machines, both of which can be and are used to infringe copyrights." In its appeal, the recording industry will argue that Wilson's analysis was flawed, citing earlier decisions in the Napster case, in which judges said that the VCR analogy (known as "substantial noninfringing use" in legal circles) does not apply if a company knows its products are being used for illegitimate purposes. "We believe (Grokster and Streamcast) are operating just like Napster and fall under the Napster ruling that the court handed down three years ago," says an attorney for the Motion Picture Association of America. "They do have one thing Napster lacked, and that is a good business model. They are making millions of dollars off of content that is not theirs." (CNet News.com 2 Feb 2004)

Category 24.9 Peer-to-peer networking

### 2004-07-07 **file-sharing peer-to-peer music sharing service colleges academia copyright** infringement intellectual property rights

NewsScan

FILE-SWAPPING AT A NEW LEVEL: I2HUB

A new file-swapping service called i2hub works only at universities with access to Internet2 -- a superfast version of the Internet created for academic use. One student who uses i2hub says: "People in legal trouble aren't aware of what they're doing or they are laughing in the face of authorities by deciding to share a ridiculous number of files. I make a minimal number of downloads from the Internet." (Wall Street Journal 7 Jul 2004) (sub req'd)

## Category 24.9 Peer-to-peer networking 2004-10-06 peer-to-peer P2P Morpheus Neonet search accelerator hops network intellectual property piracy theft music video files

NewsScan; http://news.com.com/Super-powered+peer+to+peer/2100-1032\_3-5397784.html

P2P GETS A BOOST

Streamcast Networks, owner of the Morpheus file-swapping software, is releasing an updated version that incorporates technology called Neonet to speed up the search process on peer-to-peer networks. Neonet, authored by a pair of former Harvard students, uses "distributed hash tables," which are essentially a way of taking a snapshot of where every file on the network is at a given moment and scattering bits of that information around the entire network. To find a specific file, a user's search request bounces from computer to computer across the P2P network, with each hop revealing a little more information about where the file can be found. Usually just three or four hops are necessary before the file is located for downloading. "The main benefit is that it allows you to search the entire network instead of just a local area," says Jed McCaleb, chief programmer for eDonkey, which also uses Neonet technology. "It's probably faster than the way Gnutella works, and it's definitely technically superior." Neonet creators Ben Wilkin and Francis Crick say the technology also holds promise for newer applications such as Net calling. "It can be used for all sorts of distributed computing tools, and that's where we're going to go with it," says Wilkin. "It really eliminates the need to have any centralized infrastructure."

Category 24.9 Peer-to-peer networking

### 2004-11-22 **P2P peer-to-peer Weed music legal use**

NewsScan; <http://www.wired.com/news/digiwood/0,1412,65774,00.html>

P2P GROWING LIKE A WEED

Peer-to-peer file-sharing networks, the scourge of the music industry, can also be used to promote music through software programs like Weed, which allows fans to download a song and play it three times before they're prompted to pay for it. Songs cost about a dollar and can be burned to an unlimited number of CDs, passed around on file-sharing networks and posted to Web pages. "We're trying to take the problem of unauthorized music sharing and turn it into an opportunity for everyone to participate in the music business," says John Beezer, president of Shared Music Licensing, which markets the Weed software and channels payments to the artists and distributors. Weed also encourages sharing by offering a commission to users who pass a song onto a friend who then buys it. Under the distribution scheme, the copyright owner gets 50%, Weed gets 15%, and the fan who passes the music along gets 20%. [Note: The article failed to mention where the other 15% goes.] Weed is also a participant in the P2P Revenue Engine project sponsored by the Distributed Computing Industry Association, which seeks to demonstrate to entertainment firms how they can use P2P services to make money. (Wired.com 22 Nov 2004)

Category 24.9 Peer-to-peer networking

### 2004-11-29 Kazaa music Australia peer-to-peer file sharing P2P

NewsScan; http://www.siliconvalley.com/mld/siliconvalley/10295215.htm

RECORDING INDUSTRY SUES KAZAA

Australia's recording industry has filed a lawsuit to shut down the Kazaa file-swapping network, which it calls "an engine of copyright piracy to a degree of magnitude never before seen" because it allows users to freely exchange songs, movies and TV programs without paying royalties to the copyright owners. Sharman Networks Ltd., which owns Kazaa, will argue that it not only warns users not to commit music piracy but also that it has no control over what people actually do with the "peer-to-peer" software it provides. But the recording industry points out that Sharman provide software that helps users filter pornography and viruses -- yet don't provide software to filter out files containing copyrighted material. (San Jose Mercury News 29 Nov 2004)

Category24.9Peer-to-peer networking2004-12-06peer-to-peer P2P Napster Shawn Fanning Snocap

NewsScan; http://www.zdnet.com.au/insight/software/0

NAPSTER FOUNDER SINGING A NEW TUNE

Shawn Fanning, of Napster fame, is launching a new venture called Snocap that offers technology to identify songs as they are moved around on the Net and prompt users for payment before they listen. The idea is to transform peer-to-peer music sharing into a profit-making venture for the artists and record labels through a comprehensive content registry and "fingerprinting" technology. "We're trying to build something that facilitates a high-quality service. Respecting rights holders is important, but it's all working under the assumption that everyone is trying to make as much content available as possible. The business is built on the premise that a peer-to-peer service ought to be able to launch a successful authorized system and have the breadth of content that they had available previously, or close to that," says Fanning, who adds that his technology could also be used to police file-sharing of video games, software, movies and other P2P network content. "The fingerprint technology is music specific, but fingerprinting can apply to video, etc. The rule-sets are specific to music, but those are also very easily adaptable. So our system in a general sense is very extensible, and we believe that once the music space begins to adopt the Snocap system, there will be a demand for this kind of architecture to provide content in other forms." (ZDNet 6 Dec 2004)

### 24.A Secure processors

Category 24.A Secure processors

### buffer overflow hardware microprocessor fix chip manufacturers

2004-02-22 NewsScan

CHIPMAKERS RACE TO PLUG THE BUFFER OVERFLOW PROBLEM

The next generation of microprocessors will plug the gaps that have resulted in "buffer overflow" vulnerabilities, causing Microsoft to issue repeated "critical security alerts." The buffer section of computer memory stores a finite amount of data. To exploit the flaw, hackers cause more data to be sent to the buffer than it can hold, forcing it to overflow into the next chunk of buffer memory, where they then deposit their malicious code. This leaves the computer open to attack, as demonstrated by the devastating Slammer and Blaster worm invasions in 2003. "Buffer overflows are the largest class of software vulnerabilities that lead to security flaws," says the head of one security company. The new chips will be designed to block this avenue of attack, although security experts predict that determined hackers will find other ways to insert computer viruses — for example, by making a program jump to a subsection of its own code at the wrong time, perhaps to open a data port to a hacker. (New Scientist 22 Feb 2004)

Category	24.A	Secure processors	
----------	------	-------------------	--

2004-04-12 portable computers cell phones encryption security firmware chip

NewsScan

INTEL CHIPS WILL INCLUDE HARD-WIRED SECURITY

Intel's PXA27x processors — that company's next generation of chips for cell phones and handheld computers — will include hard-wired security by means of a security "engine" placed on the same piece of silicon but separated from the area where general processing takes place. Intel wireless security manager Dave Rogers says, "Carriers want to be able to identify the handset on the network. They want to make sure nobody is doing anything malicious with that handset." Some industry-watchers remain skeptical. Gartner research analyst Michael King says of Intel's wireless plans: "They're at an early place in this marketplace. Being able to dictate standards requires that you have a commanding position and I don't think they're there yet." (AP/Los Angeles Times 12 Apr 2004)

### 25.1 Remote control, RATs, reprogramming, auto-updates

## Category25.1Remote control, RATs, reprogramming, auto-updates2004-01-14Microsoft security bulletin patch flaw vulnerability fix buffer overflow overrun<br/>remote control

### DHS/IAIP Update

MICROSOFT SECURITY BULLETIN MS04- 003: BUFFER OVERRUN IN MDAC FUNCTION COULD ALLOW CODE EXECUTION (832483).

Microsoft Data Access Components (MDAC) is a collection of components that provides the underlying functionality for a number of database operations. When a client system on a network tries to see a list of computers that are running SQL Server and that reside on the network, it sends a broadcast request to all the devices that are on the network. Because of a vulnerability in a specific MDAC component, an attacker could respond to this request with a specially- crafted packet that could cause a buffer overflow. An attacker who successfully exploited this vulnerability could gain the same level of privileges over the system as the program that initiated the broadcast request. For an attack to be successful an attacker would have to simulate a SQL server that is on the same IP subnet as the target system. A target system must initiate such a broadcast request to be vulnerable to an attack. An attacker would have no way of launching this first step but would have to wait for anyone to enumerate computers that are running SQL Server on the same subnet. Also, a system is not vulnerable by having these SQL management tools installed. Code executed on the client system would only run under the privileges of the client program that made the broadcast request. Microsoft has assigned a severity rating of "Important" to this issue.

Category 25.1	Remote control.	RATs, reprogramming,	auto-updates
---------------	-----------------	----------------------	--------------

2004-01-14 Microsoft security bulletin patch flaw vulnerability fix remote control buffer overflow

### DHS/IAIP Update

MICROSOFT SECURITY BULLETIN MS04- 001: VULNERABILITY IN MICROSOFT INTERNET SECURITY AND ACCELERATION SERVER 2000 H.323 FILTER CAN ALLOW REMOTE CODE EXECUTION.

A security vulnerability exists in the H.323 filter for Microsoft Internet Security and Acceleration Server 2000 that could allow an attacker to overflow a buffer in the Microsoft Firewall Service in Microsoft Internet Security and Acceleration Server 2000. An attacker who successfully exploited this vulnerability could try to run code of their choice in the security context of the Microsoft Firewall Service. This would give the attacker complete control over the system. The H.323 filter is enabled by default on servers running ISA Server 2000 computers that are installed in integrated or firewall mode. ISA Servers running in cache mode are not vulnerable because the Microsoft Firewall Service is disabled by default. Users can prevent the risk of attack by disabling the H.323 filter. Microsoft has assigned a severity rating of "Critical" to this issue.

Category 25.1 Remote control, RATs, reprogramming, auto-updates

2004-07-26 WiFi wireless sensor machinery construction manufacturing application

NewsScan

WIRELESS CYBERCONTROL

The use of wireless networks of sensors and machinery has been expanding rapidly in such applications as the management of lighting systems and the detection of construction defects. Recent examples include a wireless communications system to tell precisely when to irrigate and

harvest grapes to produce premium wine and a system to monitor stresses on aging bridges to help states decide maintenance priorities. Hans Mulder, associate director for research at Intel, says that systems such as these "will be pervasive in 20 years." Tom Reidel of Millenial Net comments: "The

range of potential market applications is a function of how many beers you've had," but adds: "There's a whole ecosystem of hardware, software and service guys springing up." (New York Times 26 Jul 2004)

## 25.2 Jamming

Category 25.2 Jamming

### 2004-05-17 Wi-Fi wireless PDA jamming PDA denial of service DoS

DHS IAIP Daily; http://www.newscientist.com/news/news.jsp?id=ns99995000

May 17, New Scientist — Wi- Fi networks can be jammed from PDAs.

Wi- Fi networks can be jammed using nothing more sophisticated than a PDA and an off- the- shelf wireless networking card, the Australian Computer Emergency Response Team (AusCERT) has warned. Wi- Fi networks are becoming common in workplaces and elsewhere and it was known that they are vulnerable to jamming. It was thought that this would require the use of large, powerful and expensive equipment, but students at the Queensland University of Technology have now proved this wrong. AusCERT says attacks will be hard to foil because the problem exploited is inherent in the Wi- Fi protocol. However, such an attack can only deny access to the network- - it will not enable hackers to access user's data or computers. The problem stems from how the Wi- Fi networks allocate transmission channels. As in many other networks, Wi- Fi nodes check to see if other devices are transmitting on the same frequency band before they begin sending data, to avoid "collisions" that occur when two or more devices talk simultaneously. Like a conversation among a group of people, this works well as long as all devices are well- behaved. But it breaks down if one person or one device insists on talking loudly and continually. In essence, the Wi- Fi jamming is a denial of service attack.

Category 25.2 Jamming

2004-05-18 attack spy camera wireless vulnerability PDA Quennsland University

NewsScan

ATTACK JAMS SPY CAMERAS

An electronic invisibility cloak generated by nothing more than an off-the-shelf PDA would allow intruders to elude wireless security cameras using vulnerabilities in the most common wireless technologies. There is no defense against such a Mission Impossible-style attack, which can be used to knock out wireless networks and possibly transfer unwitting users to a spoofed wireless network. Accidentally discovered last year by PhD students at the Queensland University of Technology's Information Security Research Centre, the exploit presents obvious applications for terrorism and espionage. The vulnerability is "trivial" to exploit and only took 30 minutes to master, says Associate Professor Mark Looi. "It just uses off-the-shelf hardware and you don't need to write specific software, you just need to know the correct commands to use with the software that's supplied. On a difficulty rating of 1 to 10, it's probably a 2." (The Age 18 May 2004) Rec'd from John Lamp, Deakin Univ.

### Category 25.2 Jamming

### 2004-10-11 France jamming cell phones movie theaters regulations law Europe denial-ofservice DoS suppression

NewsScan; http://apnews.excite.com/article/20041012/D85LIBC80.html

FRANCE APPROVES CELL PHONE-JAMMING IN THEATERS

Tired of chatty theater-goers disturbing your entertainment enjoyment? France Industry Minister Patrick Devedijian has approved a decision by the country's Telecommunications Regulation Authority to allow cinemas, concert halls and theaters to install cell phone jammers that would prevent patrons from making or receiving calls during performances. Devedijian stipulated that emergency calls and calls made outside theaters and other performance spaces must not be affected, however. The move comes in response to "a long-standing request" from cinemas, says Jean Labbe, president of the National Federation of French Cinemas, noting that movie theaters had invested heavily to improve comfort and that "the authorization of jammers is the cherry on the cake." (

### Category25.2Jamming2004-10-19TV remote control jamming denial-of-service DoS brute-force cryptanalysis

i v remote control jamming demai of service Dob brute force

NewsScan; http://www.wired.com/news/culture/0,1284,65392,00.html

TV-B-GONE ZAPS INTRUSIVE BROADCASTS

Inventor Mitch Altman has the answer for people in airports, doctors' offices, restaurants and bars that feature blaring television sets as part of the ambiance. The TV-B-Gone is a universal remote disguised as a tiny keychain fob that works on most televisions and comes in two models geared toward European TV sets or Asian- American ones. When activated by pressing a button, the device runs through about 200 different codes that turn off various TV models, starting with the most popular brands and then moving to the more obscure. One TV-B-Gone enthusiast notes, "You've heard about the battle for eyeballs. They're your eyeballs. You should not have your consciousness constantly invaded. Television people are getting better and better at finding ways of roping us into TV where we can't get away." Altman says friends who've heard about the device have approached him about other uses, such as one that could jam cell phones or shut down vehicle subwoofers and car alarms.

### Category 25.2 Jamming

### 2004-11-04 Ireland cell phone jamming theaters regulation law denial-of-service DoS

NewsScan; http://theage.com.au/articles/2004/11/04/1099362260997.html

IRELAND TO SILENCE MOBILES IN CINEMAS, THEATERS

Ireland's cinemas and theatres have been given the go-ahead by the country's communications watchdog to permit the use of mobile phone interceptors. Interceptors will allow the creation of "quiet zones" where the mobile phones will not ring but where calls can still be made to emergency services or to lists of approved numbers, the Communications Regulator said on Wednesday. (The Age 4 Nov 2004)

## 25.3 RFI, HERF, EMP/T

Category 25.3 RFI, HERF, EMP/T

2004-04-20 pacemakers electrical interference

NYT

http://www.nytimes.com/2004/04/20/health/policy/20PACE.html?th=&pagewan ted=print&position=

RFI CAUSES TROUBLE FOR PACEMAKERS

Users of cardiac pacemakers are finding an increasing number of devices at work and at home that interfere with their artificial heart-rate controls. The culprit is generally electrical; examples include electrical nerve stimulators (PENS) and "alternative medicine" devices such as the Zapper, which sends electrical shocks through the victim, er, patient for no obvious reason.

## 26.1 Radiation

Category 26.1 Radiation

### 2004-11-16 glaucoma computer screens sight blindness

NewsScan; http://www.msnbc.msn.com/id/6493299/

HEAVY COMPUTER USE LINKED TO GLAUCOMA

Researchers at the Toho University School of Medicine in Tokyo have found that long hours spent in front of a computer screen may increase the risk of glaucoma in nearsighted people. Glaucoma, which is caused by damage to the optic nerve, results in blind spots or visual impairments that can lead to blindness. The research is based on a study of 10,000 workers in Japan who were tested for the disease, with results correlated to data on how many hours were spent on the computer and also preexisting visual problems, such as myopia. Scientists said they believe the optic nerve in myopic people might be more vulnerable to computer-caused stress than in normal eyes. "Computer stress is reaching higher levels than have ever been experienced before. In the next decade, therefore, it might be important for public health professionals to show more concern about myopia and visual field abnormalities in heavy computer users," says the report published in the British Journal of Ophthalmology. (Reuters/MSNBC 16 Nov 2004)

### 26.2 Toxic materials

Category 26.2

### Toxic materials

### toxic dust processors monitors reproductive neurological disorders

2004-06-04 NewsScan

TOXIC DUST

A survey by environment groups called the Silicon Valley Toxics Coalition says that "toxic dust" found on computer processors and monitors contains chemicals linked to reproductive and neurological disorders. Coalition director Ted Smith says, "This will be a great surprise to everyone who uses a computer. The chemical industry is subjecting us all to what amounts to chemical trespass by putting these substances into use in commerce. They continue to use their chemicals in ways that are affecting humans and other species." However, physician Gina Solomon of the Natural

Resources Defense Council says: "The levels in the dust are enough to raise a red flag, but not enough to create a crisis. I have an old computer monitor in front of me now, and I'm not about to throw it away. But when I get a new one, it darn well will be free of these chemicals." A Dell

spokesman says, "People can be very confident about their new computer purchase. We've worked a lot with suppliers, and we require audits and material data sheets on all our products." (AP/Los Angeles Times 4 Jun 2004

### Category 26.2 Toxic materials

### 2004-11-11 nanotech EPA environment risks threats dangers biology medicine nanotubes

NewsScan; http://www.washingtonpost.com/wp-dyn/articles/A43763-2004Nov11.html

### STUDYING NANOTECH RISKS

The Environmental Protection Agency has awarded \$4 million in grants to a dozen universities to study the biological and medical implications of nanotechnology, which has already yielded such products as carbon "nanotube" electrical wires; cages of atoms that can capture pollutants in water and soil; and catalysts that reduce manufacturers' dependence upon caustic chemicals. Recognizing that these materials are small enough to enter the lungs (and perhaps even be absorbed through the skin and travel to the brain and other organs), EPA official Paul Gilman explained: "This emerging field has the potential to transform environmental protection, but at the same time we must understand whether nanomaterials in the environment can have an adverse impact." Barbara Karn of the EPA's Office of Research and Development says the projects funded by the new grants will do "infinitely more" on nanotech safety than has ever been done previously. (Washington Post 11 Nov 2004)

## 26.3 Heat

Category26.3Heat2004-06-28mobile phone health risk sperm count decrease

NewsScan

MOBILE PHONES CUT SPERM COUNT

Men who regularly carry a mobile phone could have their sperm count reduced by as much as 30% according to a new study by Hungarian researchers. Those who place their phone near their groin, on a belt or in a pocket, are at greatest risk. The research findings are the first to suggest that male fertility could be affected by the radiation emitted by mobile phones, also long suspected of causing cancer. The study found the sperm that did survive exposure to mobile phone radiation showed abnormal movements, further reducing fertility. But experts are advising men not to panic yet. (The Australian 28 Jun 2004) Rec'd from John Lamp, Deakin University

## 27.3 Intrusion detection systems

Category 27.3 Intrusion detection systems

### 2004-01-23 Florida instrusion detection systems IDS funding

### NIPC/DHS;

http://www.fcw.com/geb/articles/2004/0119/web- florida- 01- 20- 04.asp

January 20, Federal Computer Week — Florida governor seeks IT funding overhaul.

Florida Governor Jeb Bush on Tuesday, January 20, outlined a 2004-2005 budget that calls for several changes at the State Technology Office (STO), including consolidating its funds to gain better control of cross-sector initiatives. This year, the STO's Information Technology Security Office is developing a statewide intrusion detection service, or Cyber Center, using funding from a federal grant. That service "will move the office into an expanded role to provide physical monitoring of the state's IT infrastructure to detect, prevent and minimize cybercrime," according to budget documents. Governor Bush requested almost \$1.1 million of the state's money to continue the security office's work. The new budget also reflects the STO's shift from legacy systems to Web-based services. Over all of this, the budget proposes a complete reorganization of the STO's programs into a single budget. "This realignment of budget authority within a single budget entity will provide the necessary flexibility for the State Technology Office to meet the needs of its IT partners and customers as needed, while also maintaining the requisite level of budgetary accountability."

Category 27.3 Intrusion detection systems

### 2004-10-23 neural networks University of Florida

NewsScan; http://www.wired.com/news/medtech/0,1286,65438,00. Html

NEURAL NETWORK AT THE CONTROLS

Researchers at the University of Florida have created a neural network made up of 25,000 disembodied rat neurons and hooked it up to a flight simulator on a desktop computer. The neurons, which are growing on top of a multi-electrode array, are fed information about the simulated F-22's horizontal and vertical movements by stimulating the electrodes, causing them to fire in patterns that are then used to control the aircraft. "It's as if the neurons control the stick in the aircraft, they can move it back and forth and left and right," says UF professor Thomas DeMarse. "The electrodes allow us to record the activity from the neurons and stimulate them so we can listen to the conversation among the neurons and also input information back into the neural network." Thus far, the network has "learned" how to control the fighter jet's pitch and roll in a broad range of weather conditions, but DeMarse plans to improve the system by having the "brain" use a horizon to judge how well it's controlling the aircraft. The goal is to find out how the neurons communicate with each other and eventually translate that knowledge into the development of a novel computing architecture. (Wired.com 23 Oct 2004)

[MK note: of possible value for future intrusion-detection systems?]

# 27.4 Firewalls & other perimeter defenses

Category 27.4 Firewalls & other perimeter defenses

### 2004-02-20 personal firewall ZoneAlarm vulnerability e-mail attack buffer overflow

DHS IAIP Daily; http://www.eweek.com/article2/0,4149,1530946,00.asp

February 20, eWeek — ZoneAlarm bug bares system to e- mail attack.

Security vendor Zone Labs has disclosed that several versions of its personal- firewall products are vulnerable to a buffer- overflow attack. ZoneAlarm, ZoneAlarm Plus and ZoneAlarm Pro 4.0.0 versions; ZoneAlarm Pro 4.5.0; as well as Zone Labs Integrity Client 4.0.0 are vulnerable. ZoneAlarm users are advised to upgrade to Version 4.5.538.001. The problem was described by eEye Digital Security on the BugTraq mailing list. The firewalls process SMTP (e- mail) traffic sent to or from the system. According to the description, a sufficiently large value in the SMTP "RCPT TO" command can overflow a stack- based buffer in the TrueVector Internet Monitor (vsmon.exe) process. According to Zone Labs, "If successfully exploited, a skilled attacker could cause the firewall to stop processing traffic, execute arbitrary code, or elevate malicious code's privileges." An attacker with local access and restricted privileges to SYSTEM level, and a remote user could invoke the attack by manipulating the system into sending an e- mail with the overflow value. Additional information available here: http://download.zonelabs.com/bin/free/securityAlert/8.html

Category 27.4 Firewalls & other perimeter defenses

### 2004-03-31 new security hacking toolkit Cisco warning threat vulnerability

DHS IAIP Daily;

http://www.computerworld.com/securitytopics/security/story/0,10801,91748,00.html

March 29, IDG News Service — Cisco warns of new hacking tool kit.

Cisco Systems Inc. has warned customers about the public release of computer code that exploits multiple security vulnerabilities in Cisco products. Using exploits for nine software vulnerabilities, the program could allow malicious hackers to compromise Cisco's Catalyst switches or a wide variety of machines running versions of the company's Internetwork Operating System (IOS). Called the Cisco Global Exploiter, the program appears to give users a menu of choices, depending on the system they are trying to crack. It offers, for example, the "Cisco 677/678 Telnet Buffer Overflow Vulnerability" or the "Cisco Catalyst 3500 XL Remote Arbitrary Command Vulnerability," according to the Web site, www.k- otik.com. Computer code for a program matching the description in the Cisco security notice was posted on the French- language computer security exploit site yesterday. While many of the exploits can be used only to shut down affected Cisco devices in denial- of- service attacks, at least one enables remote attackers to run malicious code on the affected system without needing a username or password, according to the Cisco security notice. Customers should patch software vulnerabilities exploited by the program.

Category 27.4 Firewalls & other perimeter defenses

### 2004-08-19 Cisco Internetwork Operating System IOS vulnerability OSPF packets denial-ofservice DoS

DHS IAIP Daily; http://www.kb.cert.org/vuls/id/989406

August 19, US- CERT — Vulnerability Note VU#989406: Cisco IOS fails to properly handle malformed OSPF packets.

Cisco Internetwork Operating System (IOS) is a very widely deployed network operating system. IOS provides support for the Open Shortest Path First (OSPF) protocol. There is a denial- of- service vulnerability in the way OSPF packets are processed by IOS. By sending a specially crafted OSPF packet to an affected device, a remote, unauthenticated attacker could cause the device to reload. Repeated exploitation of this vulnerability could result in a denial- of- service condition. In order to exploit this vulnerability, an attacker would need to know several parameters. These parameters include the OSPF area number, netmask, hello, and dead timers, which are configured on the affected device. Information about upgrading is available on the Cisco Website: http://www.cisco.com/warp/public/707/cisco- sa- 20040818- ospf. Shtml

2004-08-27	Cisco Internetwork Operating System IOS telnet denial of service DoS vulnerability
Category 27.4	Firewalls & other perimeter defenses

DHS IAIP Daily;

http://www.cisco.com/en/US/products/products\_security\_advisory09186a00802a cbf6.shtml#summary

August 27, Cisco Security Advisory — Cisco telnet denial of service vulnerability.

A denial- of- service vulnerability exists in Cisco's Internetwork Operating System (IOS). This vulnerability could allow remote attackers to prevent new connections to remote management services on a vulnerable device. This vulnerability allows specially crafted TCP packets sent to the telnet or reverse telnet service to cause the device to refuse subsequent connections to these management services. There are reports of this vulnerability being actively exploited. Patches and workarounds are available through the Source link below.

Category 27.4	Firewalls & other perimeter defenses
2004-11-11	Cisco Internetwork Operation System IOS vulnerability DHCP protocol exploit denial of service DoS attack

DHS IAIP Daily; http://www.kb.cert.org/vuls/id/630104

November 11, US- CERT — Technical Cyber Security Alert TA04- 316A: Cisco IOS Input Queue Vulnerability.

There is a vulnerability in the way Cisco IOS processes Dynamic Host Configuration Protocol (DHCP packets). Exploitation of this vulnerability may lead to a denial of service. The processing of DHCP packets is enabled by default. The Dynamic Host Configuration Protocol (DHCP) provides a means for distributing configuration information to hosts on a TCP/IP network. The Cisco Internetwork Operating System (IOS) contains a vulnerability that allows malformed DHCP packets to cause an affected device to stop processing incoming network traffic. By sending a specially crafted DHCP packet to an affected device, a remote, unauthenticated attacker could cause the device to stop processing incoming network traffic. Repeated exploitation of this vulnerability could lead to a sustained denial- of- service condition. In order to regain functionality, the device must be rebooted to clear the input queue on the interface. Cisco is tracking this issue as CSCee50294. US- CERT is tracking this issue as VU#630104. A solution is to upgrade to fixed versions of IOS available at: http://www.cisco.com/warp/public/707/cisco- sa- 20041110- dhcp. Shtml

Category 27.4 Firewalls & other perimeter defenses

2004-11-19 ZoneAlarm advertising blocking vulnerability denial of service DoS

DHS IAIP Daily; http://secunia.com/advisories/13244/

November 19, Secunia — ZoneAlarm advertising blocking denial of service vulnerability.

A vulnerability has been reported in ZoneAlarm Pro and ZoneAlarm Security Suite, which can be exploited by malicious people to cause a DoS (Denial of Service). The vulnerability is caused due to an error in the Ad- Blocking feature (disabled by default) when processing JavaScript and can be exploited by tricking a user into visiting a malicious Website containing specially crafted JavaScript. Update to version 5.5.062 or later via the "Check For Update" feature.

## 27.7 Anti-malware technology

Category 27.7	Anti-malware technology
2004-03-03	antivirus scanner attachments password protection remove ZIP files security policy unintended consequences

23

24

### RISKS

UNINTENDED CONSEQUENCES OF ATTACKING VIRAL MAIL

With some viruses sending out e-mail containing password-protected attachments, some system administrators have taken to removing all password-protected attachments from inbound e-mail. Vassilis Prevalakis of the Computer Science Department at Drexel University points out that such broad-brush responses "will cause severe disruption to secure communications over e-mail." He thinks "we should resist such efforts and prevent the spammers and virus writers do to us what the government failed to do."

Category 27.7	Anti-malware technology
2004-06-18	hack-back systems retaliations iSIMS Symbiot Security

NewsScan

ATTACKING THE ATTACKERS: MAYBE NOT A GOOD IDEA

A company called Symbiot Security has created "Intelligent Security Infrastructure Management Systems" (iSIMS) that not only provide traditional defensive measures against viruses, worms, and other kinds of network vandalism -- but also offer the victims of vandalism a gradual escalation of

retaliation measures. These include the ability to flood the attacking computers with data. However, some experts say that retaliatory actions could be a very bad idea. Adrian Vanzyl of the security firm Seclarity comments: "So you are in effect breaking into each of those systems as you follow this person back. Are you legally liable for that? It's a very, very good question." And Dorothy Denning, professor of defense analysis at the Naval Postgraduate School, warns: "We've seen worms that have had major impact like causing delays in airline schedules, shutting down ATM machines, 911 systems and so on. Putting any kind of worm out there would be dangerous." (AP/San Jose Mercury News 18 Jun 2004)

Category 27.7 Anti-malware technology

2004-11-30 virus throttling HP Hewlett Packard artificial intelligence AI slowing spread worms

NewsScan;

'VIRUS-THROTTLE' SOFTWARE FROM HP

Software engineers at Hewlett-Packard are developing "virus-throttling" software to slow the spread of viruses and worms on the Internet by identifying suspicious behavior. HP chief technology officer Tony Redmond says, "Any worm or virus that depends on its ability to spread itself will be hurt by this technology." Alan Paller, director of research at the SANS Institute, says the overall idea "makes sense," and adds, "It's an arms race, not a simple war. I've been hearing people talk about the notion of throttling for a long time, and it's a spectacular idea if HP can get it to work." (Washington Post 30 Nov 2004)

## 28.1 Spyware, Web bugs & cookies

Category 28.1 Spyware, Web bugs & cookies

### 2004-01-06 anti spyware software AOL Earthlink

NewsScan

AOL JOINS EARTHLINK IN OFFERING ANTI-SPYWARE SOFTWARE

America Online will soon start offering its customers anti-spyware software, following the lead of EarthLink, which is the only other major Internet service provider to provide its subscribers with software that automatically flags programs designed to secretly track users' Internet habits. Spyware usually finds its way onto a PC when users download file-sharing software or stumble onto certain Web sites. "Spyware is an electronic stalker that secretly watches the online activities of millions of Americans every day," says AOL executive VP David Gang. "Because spyware hides in the background and quietly attaches itself to other programs, most computer users don't even realize they have it on their machines." One EarthLink exec predicts that spyware eventually will outstrip computer viruses as an online scourge, because its motivation is rooted in a quest for profits rather than random malice. (Washington Post 6 Jan 2004)

Category28.1Spyware, Web bugs & cookies2004-01-14spyware Earthlink prevention

NewsBits; http://zdnet.com.com/2100-1104\_2-5141073.html

EarthLink tool hunts down spyware

The company's Spy Audit software is intended to ferret out unwelcome programs that take up surreptitious residence on a computer's hard drive, typically when someone downloads freeware or shareware but also through e-mail and instant messaging. Those programs keep track of a computer user's online activity and can be difficult to locate and remove. Problems that arise from spyware's presence can range from the annoying --a barrage of pop-up ads--to the menacing, including the potential for data corruption and theft of personal information.

Category	28.1	Spyware,	Wel	b bugs &	& cookies			
					-	-		

### 2004-02-04 spyware insidious software detector Trojan horse SpyBan

NewsScan

DOUBLE-AGENT SPYWARE

It turns out that at least one spyware program purporting to identify and delete unwanted advertising software actually installs its own spyware software on the unsuspecting user's computer. SpyBan has been singled out for such nefarious behavior by several competing anti-spyware companies: "I classified SpyBan as a Trojan Horse, since it gives the impression that it will protect your privacy, but does the opposite — it installs spyware," says a spokesman for Sweden-based Kephyr.com. The software allegedly leaves behind a program called Look2Me, which has been identified by Symantec as a spyware application: "Look2Me is a spyware program that monitors visited Web sites and submits the logged information to a server." The SpyBan Web site was shut down after reporters started snooping into its activities, but a trace of the company's domain name indicated the site was hosted at the same address as NicTech Networks. Experts say spyware and adware software can be difficult to track down because it's designed to "hide" on the user's PC. "I doubt anyone knows precisely what these things do, apart from the authors," says a researcher for PestPatrol, a legitimate anti-spyware outfit. "They are really complex. Viruses are easy compared to these things." (CNet News.com 4 Feb 2004)

NewsScan; http://www.washingtonpost.com/wp-dyn/articles/A23307-2004Mar2.html

### SENATE BILL TARGETS SPYWARE

U.S. Senators Ron Wyden (D-Ore.), Conrad Burns (R-Mont.) and Barbara Boxer (D-Calif.) are backing a bill dubbed the "SPYBLOCK" Act, which would make it illegal to use the Internet to install software on people's computers without their consent, and would require companies that offer software downloads to provide more information about what the programs do and what information they collect. The bill also would require ads generated by spyware or adware programs to be clearly labeled as such. "Computer users should have the security of knowing their privacy isn't being violated by software parasites that have secretly burrowed into their hard drive," says Wyden. Spyware has been around for years, but as its sneaky code has reached out to touch more users, the tide of public sentiment has now turned against it. "The major concern here is user control and transparency," says Ari Schwartz, associate director for the Center for Democracy and Technology. "We've found that many consumers do not understand what they're getting themselves into when they download software." Some skeptics say this latest effort is likely to be every bit as effective as the preceding CAN-SPAM Act, which many computer experts say has done little to curb the deluge of spam flooding consumers' in-boxes. "If you apply the mailbox test, the spam law hasn't had a significant effect. It would be nice to see the spam law working as intended before we say we want to follow the same route with spyware," says one attorney. (Washington Post 2 Mar 2004)

Category 28.1	Spyware, Web bugs & cookies
2004-03-04	legislation US Senator spyware insidious software SPYBLOCK act law

NIPC/DHS

March 02, Washington Post — Senators try to smoke out spyware.

Three U.S. senators are tackling the growing problem of "spyware," software programs that track what people do online, alter their Web browser settings and turn their computers into unwitting Internet advertising generators. The "SPYBLOCK" Act, which was introduced late last week, would make it illegal to use the Internet to install software on people's computers without their consent, and require companies that offer software downloads to provide more disclosure about what the programs do and what information they collect. The bill also would require Internet ads generated by the software to be clearly labeled. The bill would allow states to sue violators in federal court and would call on the Federal Trade Commission to impose fines and civil penalties under consumer protection laws. The bill probably will not cut down on the worst kinds of spyware - programs that exploit computer security flaws to hijack Internet connections or install "dialer programs" that force the computer to call expensive online 1- 900 adult services - said Stewart Baker, an attorney in Washington, DC. In that sense, Baker said, it is a lot like the CAN- SPAM Act, which many experts said has done little to combat the problem of unsolicited bulk e- mail since it became law in January. The commission is scheduled to hold a public workshop on spyware, adware and other software on April 19.

Category 28.1 Spyware, Web bugs & cookies

### 2004-03-25 spyware insidious software spam e-mail definition US Senator Kazaa

NIPC/DHS

March 23, Reuters — Senators struggle to define computer spyware.

Programs that secretly track computer users' activities are becoming an online scourge rivaling "spam" e- mail and should be outlawed before they prompt consumers to abandon the Internet, members of the Senate communications subcommittee said Tuesday, March 23. But a bill sponsored by committee members will need to define the problem precisely to avoid outlawing pop- up ads and other annoying but essentially harmless technologies, consumer and business advocates said. Like the congressional debate about "spam" e- mail last year, much rests on the definition of what constitutes legitimate marketing activity and what should be outlawed. Some online advertisers and song- swapping networks like Kazaa place programs on users' computers to monitor their activity, or harness their processors for other activities. Other programs secretly track users' keystrokes to lift passwords and credit- card numbers, or sell "fixes" for software problems they create. A bill sponsored by Sen. Conrad Burns (R- MT) would require companies to obtain permission before installing a piece of software on a consumer's computer, and provide an easy way for the consumer to remove the software if he wished.

Category 28.1 Spyware, Web bugs & cookies

2004-04-13 home user PC infested spyware insidious software

DHS IAIP Daily; http://news.bbc.co.uk/2/hi/technology/3633167.stm

April 16, BBC News (UK) — PCs 'infested' with spy programs.

Internet provider EarthLink says it uncovered 29.5 million examples of spyware on over one million computers scanned between January and March. These are parasite programs sometimes come attached to software downloaded from the Web. The details are often included in the license agreement small print that most users click through without reading. But sometimes they do not even need your permission to download, but just bury themselves on a hard drive as you browse the Internet. EarthLink said the most common type of spyware it found was adware. These are programs that displays ads on an infected computer and also sends data about surfing habits. But it also found examples of more insidious spyware. "It's disturbing that over 300,000 of the more serious system monitors and Trojans were uncovered," said Matt Cobb of EarthLink. System monitors can surreptitiously watch what you do, steal personal information and despatch it across the web, while Trojans can allow malicious hackers to get access to a computer and steal information.

## Category28.1Spyware, Web bugs & cookies2004-04-13anti-spyware insidious software Utah law invasion privacy

NewsScan

CHALLENGE TO UTAH'S NEW ANTI-SPYWARE LAW

A new Utah law called the Spyware Control Act (banning the practice of imposing pop-up ads on Internet users as they surf the Web) is being challenged in a federal lawsuit filed by the New York advertising company WhenU.com Inc., which argues that the law violates a constitutionally protected right to advertise. WhenU provides users with free software such as games and screen savers that come with a separate program, SaveNow, that tracks Web traffic and matches a user's surfing habits with particular advertisers. WhenU says its software is installed only with permission and doesn't invade privacy. (AP/San Jose Mercury News 13 Apr 2004)

Category 28.1 Spyware, Web bugs & cookies

### 2004-04-18 spyware targetted Federal Trade Commission FTC

NewsScan

FTC TARGETS SPYWARE

The Federal Trade Commission, which championed the anti-spam legislation recently enacted by Congress, now has another Internet scourge in its sights: spyware. The agency is sponsoring a workshop today to study technical and regulatory responses to spyware, but officials caution that legislation is unlikely to be passed this year. Adware (the most common type of spyware) usually piggybacks on other programs -- most notably music file-sharing or screen-saver software -- and then tracks users' Web surfing habits, relaying that information to ad companies that then bombard the user with pop-up ads. More malicious versions of spyware track keystrokes in order to steal credit card information or identity. House and Senate bills would require users' clear consent before downloads, but FTC bureau director Howard Beales says such approaches could prove cumbersome: "The question is whether there's a way to draw a workable line. If you download a set of (updates) for Windows, it comes with a bunch of different programs. You don't want to have to go through this every time." (USA Today 18 Apr 2004)

Category 28.1 Spyware, Web bugs & cookies

2004-04-19 spyware legislation slowed market-based solution insidious software user unaware

NewsScan

### A GO-SLOW APPROACH TO SPYWARE LEGISLATION

Spyware (the generic term for software that is surreptitiously downloaded onto PCs when users are engaged in some activity such as instant messaging or surfing for music or games) comes in two major varieties: the relatively innocuous "adware" that places advertisements on people's computers, and the more insidious kind that capture user keystrokes in order to steal passwords or other private information. The Internet security firm McAfee says the number of "potentially unwanted programs" on its customers' computers grew from 643,000 in September 2003 to more than 2.5 million in March. Still, Commissioner Mozelle Thompson, a member of the Federal Trade Commission, warns against trying to solve the problem with hurried and ill-conceived legislation: "There are some kinds of practices that we may consider unfair or deceptive that we already have existing power to pursue." His alternate solution is for technology companies to develop standards for downloads that would distinguish them from spyware. Marc Rotenberg of the Electronic Privacy Information Center scoffs: "To expect that market-based solutions are going to protect the consumers, I think, is to misunderstand the problem." (Washington Post 19 Apr 2004)

Category28.1Spyware, Web bugs & cookies2004-04-19Federak Trade Commission FTC industry solutions spyware

DHS IAIP Daily; http://www.esecurityplanet.com/trends/article.php/3342471

April 19, eSecurity Planet — FTC urges industry solutions to spyware.

The Federal Trade Commission (FTC) says the solution to the invasive programs generally known as spyware is more likely to be found in better technology solutions and intensive consumer education than in either state or federal legislation. Spyware is vaguely defined and often confused by consumers with adware, which are usually legal and legitimate applications. Consumer and privacy advocates attending Monday's FTC Spyware Workshop were concerned about the growing number of programs that often surreptitiously piggyback on downloaded files; they report back Internet traffic patterns to advertisers and generate unwanted popups. Even when consumers delete the downloaded file, spyware often remains and continues to monitor the user's browsing habits. FTC Commissioner Mozelle Thompson asked industry Internet provider leaders to produce a set of best practices for the use of adware, including disclosure statements to consumers regarding what they are about to download.

Category 28.1 Spyware, Web bugs & cookies

### 2004-05-13 spyware state laws combating Utah New York California

DHS IAIP Daily;

http://www.washingtonpost.com/wp- dyn/articles/A24746- 2004May 13.html

May 13, Washington Post — States speed up spyware race.

State lawmakers' eagerness to crack down on Internet "spyware" could force the federal government to move sooner than expected to pass its own law. Only one state- - Utah- - has an anti- spyware law, but New York and California both are considering proposals. If enough states pass similar laws, businesses say the resulting "patchwork" of conflicting statutes would be almost impossible to obey, adding further pressure on Congress to act. "If the states are busy writing laws and particularly if they're writing inconsistent laws or laws that strongly interfere with certain markets, that certainly would strengthen the case for federal legislation," said Howard Beales, the Federal Trade Commission's top consumer protection official. At an April FTC hearing on 13 spyware, witnesses testified that computer users often don't know how the programs got onto their machines or how to remove them. Any national spyware law probably would preempt various state laws, much like the federal Can- Spam Act preempted tougher anti- spam laws in California and Washington. Beales said that Congress should not let the threat of state laws goad it into passing a poorly written bill.

Category 28.1	Spyware, Web bugs & cookies
2004-05-20	e-mail messages read received location DidTheyReadIt.com violating physical
	space freak people

NewsScan

IF YOU SEND IT, WILL THEY READ IT?

DidTheyReadIt.com, a new service costing \$50 a year, allows a sender of e-mail to secretly track that e-mail to see whether anyone opens it, how long the recipient keeps it open, how many times it was opened, and where geographically the recipient read it. The whole process is invisible to the person who receives the message. Mitchell Kertzman of the technology investment firm Hummer Winblad says the service "violates our electronic space in a way that's as uncomfortable as someone violating our physical space. Add this company to the long list of people who are making the Internet a less attractive place to live and work." Technology expert Esther Dyson predicts that the service "will freak people out," but Case Western Reserve University professor Youngjin Yoo thinks people will be of two minds: "You will want to know how others treat your e-mail messages even if you don't necessary want others to know how you are treating theirs."

Category 28.1 Spyware, Web bugs & cookies

### 2004-05-30 spyware browser security add-in downloads scanning software anti-malware scanner pop-up blocker freeware

WP http://www.washingtonpost.com/wp-dyn/articles/A89-2004May29.html

SPYWARE BLOCKING FROM YAHOO

Yahoo's free browser toolbar, "Anti-Spy," was announced in May 2004. Using technology from PestPatrol, the company founded by Bob Bales -- who was one of the founders of the original National Computer Security Association (NCSA) back in the late 1980s -- the software blocks spyware, provides for scanning and removal of spyware, and blocks popups. By late 2004, the product was in full production and available for IE in a free download from < http://toolbar.yahoo.com >.

Category 28.1 Spyware, Web bugs & cookies

2004-06-03 Web bugs privacy e-mail confirmation permission surreptitious covert data leakage

http://www.nytimes.com/2004/06/03/technology/circuits/03spyy.html

COMPANY ENABLES WEB BUGS IN E-MAIL

Users of DidTheyReadIt.com route their e-mail through that company's servers so that it can be converted to HTML equipped with Web bugs. The spyware-infested e-mail can then report to the sender whether a recipient has opened the message and for how long. Privacy advocates protested that the surreptitious nature of the service makes it unethical. The providers of the service said they don't care.

Category 28.1	Spyware, Web bugs & cookies
2004-08-23	virus spyware combination Websurfing information leak webcam privacy

DHS IAIP Daily; http://www.webuser.co.uk/news/57657.html

August 23, Webuser — Virus spies on surfers.

A new virus, Rbot- GR, that can spy on computer users through their webcam is circulating across the Internet. The Rbot- GR worm, which spreads through shared networks, gives hackers access to the hard drive and secret passwords, as well as the ability to spy on people in their homes and workplaces through their webcams or microphones. Graham Cluley, senior consultant for Sophos said "This takes hacking to a whole new level. If your computer is infected and you have a webcam plugged in, then everything you do in front of the computer can be seen and everything you say can be recorded." Sophos believes that the worm is evidence of a growing trend in spying on innocent computer owners and poorly protected businesses. Users are advised to keep their PC's protected against the latest threats with anti- virus software and firewalls, and unplug their webcam when not using it.

Category 28.1	Spyware, Web bugs & cookies
2004-09-02	Microsoft Windows XP operating system Service Pack 2 SP2 spyware interference update

DHS IAIP Daily;

http://www.washingtonpost.com/wp- dyn/articles/A57501- 2004Sep 2.html

September 02, Associated Press — Microsoft warns spyware could bungle update.

Microsoft is warning users of the Windows XP operating system to check for spyware before downloading the free massive security update, called Service Pack 2. Barry Goff, a group product manager at Microsoft, said some spyware could cause computers to freeze up upon installation of the update. Spyware, which typically piggybacks with downloaded software such as file- sharing programs, tracks behavior, triggers pop- up ads and can otherwise cause problems on computers. Microsoft recommends that users clean their PCs of spyware and back up their data before turning on the auto update feature that automatically downloads Service Pack 2 (SP2). People who download SP2 also may need to check whether legitimate programs, such as third- party security software, need to be updated. Research firm IDC estimates that about 260 million copies of Windows XP have been sold.

Category 28.1 Spyware, Web bugs & cookies

2004-09-08 copyright anti-spyware bills legislation proposed intellectual property crime Justice Department

NewsScan

COPYRIGHT, SPYWARE BILLS MOVE FORWARD

The House Judiciary Committee has approved two bills that would establish criminal penalties of up to three years in prison for those who install spyware on others' computers and for Internet users who copy and distribute large quantities of music or movies without permission. "We must not let Internet technologies become a haven for criminals," said Rep. Lamar Smith (R-Texas). The copyright bill includes provisions for training federal agents to investigate intellectual-property crimes and would set up a Justice Department program to education the public about copyright rules. Both bills now head to the House floor for consideration; the Senate approved similar legislation in June. (Reuters/New York Times 8 Sep 2004)

2004-10-12	spyware FTC lawsuit prosecution Wallace popup windows privacy hacking
Category 28.1	Spyware, Web bugs & cookies

 $NewsScan; http://news.com.com/From+spam+king+to+spy+master/2100-1032\_3-5406348.html$ 

SPYWARE IN FTC'S CROSSHAIRS

The Federal Trade Commission is launching an aggressive new strategy to prosecute "spyware" perpetrators, and last week filed a civil lawsuit against former spam-king Sanford Wallace and his companies, Seismic Entertainment Productions and SmartBot. Wallace, who was once dubbed "Spamford" for his earlier misdeeds, operates the PassItOn.com Web site, which requires visitors to click through multiple pop-up windows in order to exit. In an interview with CNet last year, Wallace defended his practice of collecting personal information from people who visited his site: "We don't violate anybody's privacy; everything is disclosed. We're giving something away for free in exchange for consumers' permission to use private information. It's no secret. Publishers Clearinghouse has been doing this type of thing for years." However, an FTC investigator says Wallace's actions go far beyond informationgathering, by changing the home page of her Internet Explorer browser and using programming code to pop open the CD drive in her computer while displaying a message saying, "If your cd-rom drive opens... you desperately need to rid your system of spyware pop-ups immediately." Of course, the site then offers to sell a product called Spy Deleter. Anti-spyware activist Ari Schwartz says the FTC has "built a good case. This fits into the kinds of cases where FTC could get their feet wet on this issue."

Category 28.1 Spyware, Web bugs & cookies

2004-10-18 spyware adware proxy servers blocking installation prevention screening

NewsScan; http://online.wsj.com/article/0 (sub req'd)

NEW SOLUTIONS TO SPYWARE INVASION

Two companies have just released software programs aimed at eliminating the scourge of spyware. Blue Coat Systems, which specializes in proxy servers, is enhancing its security service with spyware- and adware-blocking software. It estimates that its product can prevent 98% of such unwanted programs from being installed. Webroot Software boasts a similar success rate with its anti-spyware software, which is installed directly on users' PCs. These two new products are notable because, while there are many products on the market that can remove spyware and adware from users' PCs, these two prevent their installation in the first place. Meta Group analyst Peter Firstbrook predicts that what ultimately will evolve is a "layered" defense system that combines centralized screening tools plus desktop software, similar to what's happened in the antivirus software market.

Category 28.1 Spyware, Web bugs & cookies

2004-11-15 **cookies advertising web privacy service surfing history** 

NewsScan; http://www.nytimes.com/2004/11/15/technology/15ecom.html

NEW AD SERVICE TRACKS SURFING HABITS, MAINTAINS PRIVACY

Tacoda, based in New York, is touting its new online marketing service, which directs ads to Web site visitors based on their surfing history. No personal information is sought or collected -- AudienceMatch simply traces the path of a single computer through its network of 60 Web sites, using a cookie. "This is different than what DoubleClick was trying to do," says Tacoda CEO David Morgan. "This system uses no personally identifiable information, and no data is shared between publishers. Privacy is one of the biggest issues that will drive the success of this." Tacoda's Web network comprises 60 publishers that are visited by some 100 million people monthly, or about 75% of the U.S. Internet audience. Morgan compares AudienceMatch to Google's AdSense program, which allows marketers to bid for the right to position their text messages next to stories that have a related "theme." With AudienceMatch, however, advertisers bid not on keywords, but on preset groups, like "gadget geeks," or "car buyers." Gartner analyst Denise Garcia says AudienceMatch "enables advertisers to reach a lot more people with targeted ads, which, for them, is the next big wave." (New York Times 15 Nov 2004)

## **28.2** Scumware

Scumware

Category 28.2

### slimeware AOL instant message IM software game adware

2004-02-13 NewsScan

SLIMEWARE?

Some AOL subscribers have received messages seeming to be from friends but linked to a humorous Osama bin Laden game that surreptitiously installs another program which in turn broadcasts an ad from the infected computer to all correspondents on its buddy lists. AOL executive Andrew Weinstein calls the software that does this "a particularly slimy form of adware," though the makers of that software, called Buddylinks, insists: "Our games interact with instant messengers by promoting the game among the user's network of buddies. Please understand, our flash games are in no way a virus. We simply combine peer-to-peer, social networking, and instant messaging into one spectacular technology." AOL's Weinstein says, "The one important thing for consumers to know is that they should always execute extreme caution before downloading or installing any program unless they're absolutely sure why they got it." (San Jose Mercury News 13 Feb 2004)

Category 28.2 Scumware

2004-08-10 adware scumware spyware insidious sofware personal computer ISP scan audit

NewsScan

AUDIT IDENTIFIES TOP ADWARE THREAT

A six-month audit carried out by an ISP and a software company has concluded that CoolWebSearch is one of the top adware threats on the web. The survey was carried out by the Atlanta-based ISP Earthlink and Webroot Software, the latter a company that makes privacy protection software. Slightly over two million scans were carried out during the period January 1 to June 30 this year. A total of over 54 million instances of spyware were found. CoolWebSearch's most common exploit is to hijack a user's homepage and direct it to a paying client's Web site. Damaging CWS variants can pop up so many ads that a computer locks up or crashes. (The Age, 10

Aug 2004) rec'd from John Lamp, Deakin U.

## 28.3 Keystroke loggers

Category28.3Keystroke loggers2004-03-24first civil wiretapping case California key logger Key Katcher

NewsScan

WIRETAP CASE FOCUSES ON KEYSTROKE RECORDING DEVICE

A California man has been charged with one count of wiretapping, becoming the first person in the U.S. to be charged with illegally using an electronic device to record someone's keystrokes. Larry Lee Ropp allegedly plugged a "Key Katcher" into the computer of a secretary at the insurance company where he worked. Key Katchers are commercially available and are marketed to parents who want to monitor their children's computer use. However, they are not legal when used on commercial property and when Ropp was fired for violating his company's time-clock policy, he called an employee and asked her to remove what he called a "toy" from the secretary's computer. Ropp was charged with wiretapping after the firm's technology department looked into the matter. A conviction could result in a maximum five-year prison sentence. (Los Angeles Times 24 Mar 2004)

Category 28.3 Keystroke loggers

#### 2004-05-11 hacking eavesdropping keyboards hardware

DHS IAIP Daily; http://searchsecurity.techtarget.com/originalContent/0,28914 2,sid14 gci963348,00.html

May 11, SearchSecurity.com — 'Whispering keyboards' could be next attack trend.

Eavesdroppers can decipher what is typed by simply listening to the sound of a keystroke, according to scientist Dmitri Asonov at this week's IEEE Symposium of Security and Privacy in Oakland, CA. Each key on computer keyboards, telephones and even ATM machines makes a unique sound as each key is depressed and released, according to the paper titled "Keyboard Acoustic Emanations." All that is needed is about \$200 worth of microphones and sound processing and PC neural networking software. Today's keyboard, telephone keypads, ATM machines and even door locks have a rubber membrane underneath the keys. "This membrane 11 acts like a drum, and each key hits the drum in a different location and produces a unique frequency or sound that the neural networking software can decipher," said Asonov. Asonov found that by recording the same sound of a keystroke about 30 times and feeding it into a PC running standard neural networking software, he could decipher the keys with an 80% accuracy rate. He was also able to train the software on one keyboard to decipher the keystrokes on any other keyboard of the same make and model. Good sound quality is not required to recognize the acoustic signature or frequency of the key. In fact, Asonov was able to extract the audio captured by a cellular phone and still decipher the signal.

# 28.4 Cell/mobile phones/GPS (as tracking devices)

## Category 28.4 Cell/mobile phones/GPS (as tracking devices) 2004-08-18 cell mobile phone clone tracking device South Korea electronic serial number ESN Find-Friend service

DHS IAIP Daily;

http://english.chosun.com/w21data/html/news/200408/200408180 039.html

August 18, The Chosum Ilbo (South Korea) — Cloned cell phones used to trace personal locations.

The Ministry of Information and Communication (MIC) in South Korea has said that a total of 1,940 cloned phones were detected since last November. According to the MIC, cloned cell phones might help an unscrupulous person register himself as a friend of a targeted phone owner to trace his whereabouts. Every cell phone has a unique factory- set electronic serial number (ESN) and a cloned phone is one illegally programmed to have the identical ESN to the legitimate phone. After cloning, both the legitimate and the fraudulent phones have the same ESN and phone number, and cellular systems cannot distinguish the cloned cell phone from the legitimate one. This enabled the start of the Find- Friend service, a location- based service (LBS) provided by the nation's mobile operators, which was possible only after being explicitly agreed to by legitimate phone owners. Fraudulent phone holders are able to give their consent to mobile operators.

Category 28.4 Cell/mobile phones/GPS (as tracking devices)

#### 2004-10-04 mobile cell phone hacking attack vulnerabilities spying eavesdropping

DHS IAIP Daily; http://news.bbc.co.uk/1/hi/technology/3712816.stm

October 04, BBC News — Latest mobiles open to attack. The latest generation of mobile phones is vulnerable to hackers, security experts have warned.

The warning was at an international conference on computer security in the Malaysian capital, Kuala Lumpur. According to the meeting's organizer, Dylan Andrew, loopholes in the software could allow hackers to scroll through a phone's address book by remote control and even eavesdrop on conversations. The mobile industry is aware of these security issues, said Sal Viveros, director of wireless security at McAfee. "I don't think people need to be too alarmed, but they should start asking their mobile operators to provide them with protection," he said.

#### **RFID** tags **28.6**

Category 28.6 RFID tags 2004-01-25 radio frequency identification RFID IBM Philips logistics tracking

NewsScan

IBM AND PHILIPS TEAM UP ON RFID TAGS

IBM and Philips Electronics are moving ahead on an emerging computer-based logistics system that is expected to help retailers reduce their inventory-tracking costs. Philips will manufacture the RFID (radio frequency identification) tags that can be attached to items ranging from clothes to milk cartons, while IBM will provide the computer services and system. Analysts predict that in a few years' time, RFID tags will come down in price to just a few cents apiece or less, and will be capable of storing information such as a product description, packaging and expiration dates, color and price. Research groups say that excess inventory of consumer goods and retail items valued at \$40 billion is in the supply chain at any given time and they estimate that use of advanced tracking systems such as RFID could help reduce theft and excess inventory levels by 25%. According to Applied Business Intelligence, the RFID market could reach \$3.1 billion by 2008, while IDC estimates that retail demand alone will be \$1.3 billion within four years. (Reuters/CNet News.com 25 Jan 2004)

Category 28.6 RFID tags

radio frequency ID RFID FDA tags prescription drugs

2004-02-19 NewsScan

FDA CALLS FOR RFID TAGS TO TRACK DRUGS

A report released last week by the U.S. Food and Drug Administration calls RFID (radio frequency identification) tags as the most likely technology to spur "mass serialization" of prescription drugs, which it describes as "assigning a unique number (the electronic product code or EPC) to each pallet, case and package of drugs and then using that number to record information about all transactions involving the product." A unique number would act as an "electronic pedigree," guaranteeing information on the drug's authenticity, where it was intended for sale and whether it was previously dispensed. The agency has presented plans to test and adopt RFID tracking throughout the prescription drug industry, with feasibility studies slated for this year and full scale rollout at the case and pallet level by 2007. Wal-Mart stores plans to get a head start, using RFID tags to track all controlled substance medications dispensed by its pharmacies this year. (Computerworld 19 Feb 2004)

Category 28.6 RFID tags

#### 2004-03-02 currency security features RFID urban myth hoax microwave explode burn

RISKS; http://www.prisonplanet.com/022904rfidtagsexplode.html

24

23

RFID TAGS IN \$20 BILLS? EXPLODING IN MICROWAVES?? WHO KNOWS???

A controversy, ah, exploded in March 2004 when "prisonplanet.com" published an article from two anonymous contributors claiming that new \$20 bills from the US Treasury contain an RFID tag positioned in the image of Andrew Jackson's right eye. Carrying a stack of such bills sets of RFID detectors in stores, said the letter; wrapping them in aluminum foil prevented detection. Microwaving the bills in a stack in a microwave caused all the RFIDs to explode.

Skeptics pointed out that the publisher had to back off and write, "We want to make it clear that \$20 bills will only 'pop' or 'explode' in certain microwaves." Critics suggested that the image shown on the Web site seems to consist of \_old\_, not new, \$20 bills (that is bills not containing the security features described in <

http://www.globalsecurity.org/security/library/news/2003/10/sec-031009-usia02.htm >).

The discussion then devolved into name-calling and insults.

[MK comment: this debacle could have been avoided by running controlled trials with old used \$20 bills, old unused \$20 bills, new used \$20 bills and new unused \$20 bills. Microwaving some used and unsused dollar bills might have provided useful information too. Comparing the effects of stacks of such different sorts of bills on RFID detectors would not have exceeded human capabilities either.]

Category28.6RFID tags2004-03-05radio frequency RFID tags privacy consumer profiling issues

NewsScan

WILL RFID TAGS TAG BOOKS OR READERS?

Radio frequency identification (RFID) tags — tiny devices that broadcast data about any object in which they're embedded — have been proposed as a way of improving inventory control in San Francisco's library system; however, some critics of RFID technology fear that it will be used as an invasion of the personal privacy of library patrons. Ann Brick of the ACLU says, "Privacy is really the handmaiden of the First Amendment," and Lee Tien of the Electronic Frontier Foundation warns: "Now is the time to seriously worry about the government using RFIDs to track people." But Kathy Lawhun, chief of the city's main library and a proponent of the RFID proposal, suggests that the critics are getting way ahead of themselves: "RFID is simply a chip with an antenna. You can have as little or as much as you want on that chip." (AP/USA Today 5 Mar 2004)

Category 28.6 RFID tags

#### 2004-05-03 **RFID ID air travel Transportation Security AuthorityTSA**

DHS IAIP Daily;

http://releases.usnewswire.com/GetRelease.asp?id=132-0503200 4

May 03, U.S. Newswire — TSA announces eight airports participating in Access Control Pilot Program.

Rear Adm. David Stone, Acting Administrator for the Transportation Security Administration (TSA), on Monday, May 3, announced that eight airports have been selected to participate in TSA's Access Control Pilot Program which will test Radio Frequency Identification (RFID) technology, Anti- Piggybacking technology, advanced video surveillance technology and various biometric technologies. The airports are Boise Air Terminal/Gowen Field Airport (BOI), Boise, ID; Miami International Airport (MIA), Miami, FL; Minneapolis- St. Paul International Airport (MSP), Minneapolis, MN; Newark International Airport (EWR), Newark, NJ; Savannah International Airport (SAV), Savannah, GA; Southwest Florida International Airport (RSW), Ft. Myers, FL; T. F. Green State Airport (PVD), Providence, RI; and Tampa International Airport (TPA), Tampa, FL. TSA has developed a two- phase pilot program starting with Phase I, including these initial eight airports testing various off- the- shelf biometric technologies under a variety of real- world operational environments in an effort to provide unbiased evaluations of their suitability of use.

Category 28.6 RFID tags

#### 2004-07-02 radio frequency identification tags job loss unemployment

NewsScan

RFID COULD COST 4 MILLION JOBS BY 2007

The Yankee Group, a prominent market research firm, is predicting that RFID tags will cost four million U.S. jobs by 2007, throughout numerous industries. (RFID stands for Radio Frequency Identification, a technology embedded for inventory and tracking purposes into products, materials, and shipments.) However, Yankee Group analyst Adam Zabel thinks that most workers who lose their jobs due to increased efficiencies made possible by RFID technology will be able to obtain 'more value-added' positions. (Vnunet 2 Jul 2004)

Category 28.6 RFID tags

#### 2004-07-12 radio frequency identification RFID schoolchildren Japan privacy

NewsScan

RADIO KIDS IN JAPAN

School officials in the Japanese city of Osaka will soon be using RFID technology to monitor the movements of their pupils. (The acronym stands for radio frequency identification.) The tags, which will be read by readers installed at various key locations throughout a school, will be placed on the children's schoolbags, name tags, or clothing. (CNET 12 Jul 2004)

2004-07-14	radio frequency identification RFID employees Mexico corruption scanner
Category 28.6	RFID tags

NewsScan

GOT YOU UNDER MY SKIN: RFID USED TO TAG EMPLOYEES

RFID tags have been implanted under the skin of Mexico's top federal prosecutors and investigators to give them quick access to restricted areas inside a new federal anti-crime information center. The chips also could provide more certainty about who accessed sensitive data at any given time. (In the past, the biggest security problem for Mexican law enforcement has been corruption by officials themselves.) The microchip tags lie dormant under the skin until read by an electromagnetic scanner, which uses a technology known as radio frequency identification (RFID) that's now commonly used for inventory control. (San Jose Mercury News 14 Jul 2004)

Category 28.6 RFID tags

### 2004-10-13 radio frequency identifier implant microchip FDA medical RFID patient pets access control

NewsScan; http://apnews.excite.com/article/20041013/D85MJ8I83.html

FDA APPROVES MEDICAL MICROCHIPS

The Food and Drug Administration has okayed an implantable radio frequency microchip that can transmit information on a patient's medical history to doctors in the event of an emergency. VeriChips, made by Applied Digital Solutions, are already in use as a way to track wayward pets and livestock, and nearly 200 people working in Mexico's attorney general's office have had the chips implanted in order to access secure areas. The tiny chips, which are embedded under the skin with a syringe, are programmed with a code similar to the UPC codes on retail goods, which releases patient-specific information on such issues as allergies and prior treatments when scanned.

Category 28.6 RFID tags

#### 2004-10-14 **RFID** radio freqency identifier Vatican books library anti-theft inventory

NewsScan;

http://www.cnn.com/2004/TECH/10/14/spark.rfid.vatican/index.html

VATICAN TAPS RFID TECHNOLOGY TO TRACK BOOKS

The Vatican Library has tagged about 30,000 of its books with RFID (radio frequency identification) tags since last year, and says plans call for tagging 2 million of the 40- million piece collection in the near future. That would enable the staff to complete the library's annual inventory in less than a day -- a task that previously forced it to close for a whole month. Emilia Di Bernardo, VP of Seret, the company that installed the RFID system, says initially the Vatican staff were interested only in an efficient inventory process. "But we came up with something that is not only an inventory but a way to manage the books. This way staff always know where all the books are." Di Bernardo says it is relatively inexpensive to maintain the system and the technology does not harm the books in any way. "The most expensive part is the tags and the hardware." The RFID tags cost between five and 10 cents each, but Texas Instruments, which manufactures the tags, anticipates the costs coming down. "It's robust and as the price comes down, you will see it being used more and more, including in bus ticketing and concert ticketing," says a TI spokesman.

Category 28.6 RFID tags

#### 2004-10-21 **RFID** radio freqency identifier passport

NewsScan; http://www.wired.com/news/privacy/0,1848,65412,00.html

U.S. PASSPORTS GET CHIPPED

Beginning in January, diplomats and U.S. State Department employees will be issued passports containing embedded RFID chips that will contain the individual's name, address, date and place of birth, and a digital photo. Ordinary citizens applying for new passports will get the high-tech version starting in the spring. Civil liberties advocates have called the new passports a "privacy horror," and point out that even if the data were encrypted (and it's not), it would still be very easy to steal. "If 180 countries have access to the technology for reading this thing, whether or not it is encrypted, from a security standpoint, that is a very leaky system," says Electronic Frontier Foundation attorney Lee Tien. "Strictly from a technology standpoint, any reader system, even with security, that was so widely deployed and accessible to so many people worldwide will be subject to some very interesting compromises." Meanwhile, a travel privacy expert says that in addition to identity thieves, commercial travel companies, including hotels, will capture the data when people check in or exchange currency. Intel RFID expert Roy Want says those fears are overblown, but acknowledges some theft is possible: "In principle someone could rig up a reader, perhaps in a doorway you are forcing people to go through. You could read some of these tags some of the time."

### Category28.6RFID tags2004-10-21privacy VeriChip consumers Dixon RFID radio frequency identifier

NewsScan; http://www.christiansciencemonitor.com/2004/1021/p13s01-stct.html

DESCENT FROM PRIVACY: A 'SLIPPERY SLOPE'

Pam Dixon, executive director of the World Privacy Forum, warns: "Most consumers don't fully understand the tradeoffs they're making with privacy." As an example, she argues that the potential widespread use of the VeriChip -- a tiny radio transmitter inserted under a person's skin -- is "a nightmare situation" for privacy, because at first workers might be induced to wear the devices simply to get high-security jobs but that eventually the transmitters would be much more broadly required: "All of a sudden it becomes mandatory for certain classes of people. I just see this as an extremely slippery slope." (Christian Science Monitor 21 Oct 2004)

#### Category 28.6 RFID tags

### 2004-11-19 **RFID** radio freqency identifier FDA medical surgery SurgiChip identification patient quality assurance error avoidance

NewsScan; http://www.siliconvalley.com/mld/siliconvalley/10226986.htm

MAKE INCISION HERE: RFID TAG USED IN SURGERY

The U.S. Food and Drug Administration has approved use of radio frequency ID (RFID) tags to ensure that physicians perform the right surgery on the right patient. Manufactured by SurgiChip Inc., the radio tag is encoded with the patient's name and the site, type, and date of the surgery; the patient helps stick the adhesive-backed tag near the site of the surgery and workers in the hospital's operating room scan the tag to compare that information with the patient's chart. (AP/San Jose Merury News 19 Nov 2004)

## Sociology of cyberspace

Category 29	Sociology of cyberspace
2004-07-31	weblog blog Internet writing Webpage disintermediation business information
	security customer partner sharing

NewsScan

29

BUSINESS BLOGGING GOES MAINSTREAM

Major technology companies such as Microsoft and IBM are endorsing blogging as a means of enhancing companies' communications channels while at the same time eyeing them as potential profit-boosters. At a recent conference held at the University of California Berkeley's Haas Business

School, IBM Almaden Research Center director James Spohrer outlined his company's plans for integrating blogging into its employee communication strategies: "It's about decreasing social space between employees, and increasing the amount of knowledge shared between people." An example might contain some of an individual's educational background and work experience, as well as information on product development strategies that colleagues and customers can access around the clock. This sharing of information could spur feedback on efforts to produce new products and improve business processes, said Spohrer. Meanwhile, some analysts are looking at the marketing potential inherent in blogging. "Blogs are a way to put a human face on the company," because of the continuous interaction and relationships that employees can develop with blog-readers, says Forrester Research analyst Charlene Li. (Reuters 31 Jul 2004)

### 29.1 Addiction, games & violence

Category 29.1 Addiction, games & violence

#### Internet addiction usage monitoring employee usage IT addition

2004-04-28 NewsScan

COFFEE CAN WAIT -- GIVE ME MY NET!

Given the choice between going online or enjoying a morning cup of coffee, almost half of workers polled (49%) say they'd forgo the java, according to a survey by Websense. But the response signals trouble ahead for employers, who fear that productivity is suffering as a result of workers' Net addiction. While 51% of employees surveyed said they spent only about two hours a week on personal Web surfing, IT managers pegged the number at a far higher six-plus hours a week. IT managers also expressed concern over network security when employees took their laptops home with them. "Some employees take their laptops home and use their own time to download a movie. They may access a site where there's spyware or a virus and then they bring their laptop back to work and don't realize they've exposed people on their network," says Kian Saneii, VP of marketing at Websense. (CNet News.com 28 Apr 2004)

Category 29.1	Addiction, games & violence
2004-07-08	Iraq war image picture JPEG online news newpapers graphic viewership Americans US

NewsScan

AMERICANS FLOCK TO GRAPHIC WAR IMAGES ONLINE

About one in four American Internet users sought out graphic war images that were deemed too gruesome to display in conventional media such as newspapers and television, according to new research by the Pew Internet Project. The results were drawn from a telephone survey conducted between May 14 and June 17 -- a period that encompassed such disturbing events as the murder and dismemberment of American contract workers in Fallujah, the exposure of prisoner abuse at Abu Ghraib, and the capture and beheading of U.S. civilian Nicholas Berg. Survey respondents reported mixed feelings after viewing the images -- 51% said they felt they'd made a good decision to access the images, but a third said they wished they hadn't seen them. "Millions of Internet users want to be able to view the graphic war images and they see the Internet as an alternative source of news and information from traditional media. But many who do venture outside the traditional and familiar standards of the mainstream news organizations to look at the images online end up feeling very uncomfortable," says report co-author Deborah Fallows. Women in particular seemed more troubled over the entire issue of graphic online images, while younger adult Internet users tended

to approve their availability. (Pew Internet Project News Release 8 Jul 2004)

Category	29.1	Addicti	ion, ga	mes & v.	iolence		

### 2004-08-02 cyber life trend academia college university student lifestyle Internet IM surfing laptop brain information storage retrieval

NewsScan

JUST A MINUTE -- MY BRAIN IS BOOTING UP

Increasingly, college students are toting their laptops to class and using them as retrieval mechanisms for information they haven't yet managed to store in their carbon-based brain cells. The phenomenon was predicted 40 years ago by Marshall McLuhan, who suggested that people's senses were extending outside of their bodies, in the way a book was an extension of the eye and a car was the extension of a foot. Internet researcher Sherry Turkle has documented this latest evolutionary trend in her book "Life on the Screen" where she describes a typical college student's study habits -- the text book is open, the CNN news ticker is flickering across the TV screen, the headphones are pumping out the latest alternative rock, and the student's fielding IM messages as he/she surfs the Web. "Real life is just one more window," says one multitasking student. (CNN.com 2 Aug 2004)

<i>Category 29.1</i> 2004-08-04	Addiction, games & violence conscripts Finland army military draft Internet addiction unfit serve			
NewsScan				
FINLAND DISMISSI	NG 'NET-ADDICTED' CONSCRIPTS			
A growing number of conscripts have to be dismissed from Finland's armed forces every year due to an Internet addiction that makes them unsuited for service. A Finnish official says: "It's an increasing problem. More and more young people are always on the Internet day and night. They get up around noon and have neither friends nor hobbies. When they get into the army, it's a shock to them." There are no specific figures and the military has yet to give the condition a proper dismissal code in its health records. (The Age, 4 Aug 2004) Rec'd from J Lamp				
Category 29.1 2004-08-07	Addiction, games & violence sociology cyberspace psychology disorder Website Internet e-commerce marketing			

NewsScan

A SICK TRADE

The phenomenon of weborexics first became apparent about three years ago with the emergence of so-called pro-ano, or proanorexia, Web sites. But they've taken a sinister turn, with several sites cashing in by selling pro-ano merchandise, including teddy bears, "ana" bracelets and tank tops with slogans such as "nothing eaten, nothing gained." Pro-anos are one of the more disturbing online communities because of their promotion of anorexia as a lifestyle choice and badge of honor. The Web sites typically contain a weight-loss weblog, a how-to guide with tips on starving and purging, and "trigger pictures" of thin celebrities. Many of the homepages and forums have been disabled but a plethora of sites can still be easily found. Anorexics can now go online and for between \$3 and \$25 buy a red-beaded "ana" bracelet -- a symbol of solidarity that identifies them to the rest of the community. The bracelets are designed to help anorexics resist their hunger by being worn on the hand used to eat with. (The Age 7 Aug 2004) rec'd from John Lamp, Deakin U.

Category 29.1 Addiction, games & violence

#### technology syndrome Internet e-mail cell phone PDA Britain

2004-08-09 NewsScan

TECHNOLOGY CAUSING 'FRANTIC LIFE SYNDROME'

Working women in the U.K. think new technology makes their lives even more hectic, according to a new report. The advent of mobile phones and e-mail have left women feeling under greater pressure to juggle work and home commitments, leaving less time for themselves. As a result, a growing number of career women are suffering from what has been dubbed "frantic life syndrome." Research conducted for Good Housekeeping magazine found 30% of working females had regularly been driven to exhaustion by work and home commitments. The problem is even more acute for those living in London, where the figure rises to 47%. Some of the biggest gripes are on the subject

of technology designed to make life easier. (The Age 9 Aug 2004) Rec'd from J Lamp

Category 29.1 Addiction, games & violence

#### 2004-08-13 technology addiction family life children kids study sruvey

NewsScan

TECHNOLOGY KEEPS U.K. KIDS AWAY FROM FAMILY LIFE

British children are interacting less and less with their families and spending more time in their bedrooms watching television or playing computer games, according to a study published on Friday. Three-quarters of Britain's 11-14 year-olds have a television in their bedroom, almost two-thirds a DVD player or video recorder, and a quarter have a computer in their room, market research firm MINTEL said. Two-thirds of those surveyed said they played computer games in their rooms, and one in three said they only ever played the games alone. "Many of today's children now seem to be

experiencing greater isolation from family life," MINTEL consumer analyst Jenny Catlin said. "Sadly, it does seem that in many cases modern technology has now replaced the family unit, so that everyone does whatever they want, when they want, even if it means doing it on their own." (The

Age, 13 Aug 2004) rec'd from John Lamp, Deakin U.

## Category 29.1 Addiction, games & violence 2004-12-09 sociology virtual addiction Greenfield chats instant messaging games hyperstimulation children adolescents teenagers

NewsScan; http://www.latimes.com/technology/ats-ap\_technology10dec09

#### GET UNPLUGGED

Enough is enough, say experts who think young people need to get a life beyond the Internet. Psychologists Michelle Weill and Larry Rosen write, "It's like being lost in space. You get lost in the world of the Internet, games or multiple instant-message chats." Dave Greenfield, another psychologist specializing in high-tech issues argues: "Until technology gets 'stupid simple,' equivalent to turning on a light or a television set, it's going to eat time and energy. Do I have the right adapter? Or the right battery? Or cable?" Noting that many people buy the latest high-tech gizmos whether they need them or not, Greenfield says: "It points to a larger theme in our culture -- that new things are good and better, and that more is better, and faster is better. And that's not always the case." He's the author of a book called "Virtual Addiction." (AP/Los Angeles Times 9 Dec 2004)

## **29.3 Digital divide**

Category 29.3 Digital divide

#### Internet rural usage technology cyberspace

#### DHS IAIP Daily;

2004-02-19

http://www.cnn.com/2004/TECH/02/18/hln.wired.rural.internet/ index.html

February 19, CNN — Rural Internet use on the rise.

More rural Americans are surfing through cyberspace than ever before. Fifty- two percent of rural adults were connected in 2003, up from 41 percent in 2000. Despite the growth, rural users still lag more than 10 percentage points behind their urban and suburban counterparts, according to the latest report from the Pew Internet and American Life Project, "Rural Areas and the Internet." Why the gap? First, it's typically easier to get online in urban and suburban communities, and users have more choices when it comes to accessing the Internet. Other factors include lower income levels and the fact that rural users are often older than urban and suburban users. The majority of the analysis from the "Rural Areas and the Internet" report came from random phone surveys conducted between March and August 2003. The report is available online: http://www.pewinternet.org/

Category 29.3 Digital divide

2004-04-28

#### IT industry workers age old people skill set changing

NewsScan

RULES TO CHANGE IN 'YOUNG MAN'S' IT GAME

A new report by Australia's Swinburne University researchers has highlighted the under-representation of older people working in the IT industry, with figures showing that workers aged 45 years and over made up only 23% of the IT workforce in 2001. The study shows that only 5% of IT workers were aged between 55 and 64 (compared with 21% in the business and property services industry), and that younger males were the most likely group to work full-time in permanent employment, while women aged over 45 years were the least likely. Libby Brooke of Swinburne thinks that the dramatic drop-off in the number of people in the IT industry after the age of 45 could be attributable to a range of issues (including the recent soft jobs market and the "constantly changing skills base" within the IT industry) and says that the main question is: "How can older workers continue to be skilled and supported in the workplace?" (The Age, 28 Apr 2004)

Category 29.3 Digital divide

#### 2004-07-25 computer usage minimum age study debate technology proliferation

NewsScan

COMPUTER KIDS: HOW YOUNG IS TOO YOUNG?

There's a growing debate about whether children should be exposed to technology when they are still infants. Author Jane M. Healy opposes the practice and says, "Mental ability is gained from manipulating the three-dimensional world at that age and managing your own mind and not

having it managed by an electronic machine"; she recommends that kids stay off computers until age 7. David Elkind, professor of child development at Tufts University, has similar concerns: "Children miss out on all these basic learning experiences if they are so attuned to the virtual world." But other scholars hold the opposite view: Yong Zhao, a professor of educational psychology at Michigan State University, bought his daughter an iMac before she turned 1 and allowed her to simply bang on the keyboard to learn how the banging led to changes on the screen. And still other technology experts say the right answer lies somewhere in the middle of those two positions. Peter

Grunwald, whose consulting firm specializes in kids and technology, says: "Kids need a good balance in their lives and a mix of experiences"; his position is that computers can help kids develop hand-eye coordination and other skills, but shouldn't be used as robotic baby-sitters that shield a

child from the real world. (AP 25 Jul 2004)

## Category29.3Digital divide2004-10-28survey politics Internet digital divide sociology diversity

NewsScan; http://www.pewinternet.org/

INTERNET BROADENS VOTERS' POLITICAL HORIZONS

More than 40% of U.S. Internet users have gotten news and information about this year's presidential campaign online, and 31% of broadband users now cite the Net as their primary source of campaign news -- about the same number as those who rely on newspapers (35%). And while some pundits had expressed concern that wider use of the Internet would result in a decreased exposure to viewpoints that conflict with users', it turns out that Internet users have a greater overall exposure to political arguments, including those that challenge their preferences. "People are using the Internet to broaden their political horizons, not narrow them," says Kelly Garret, coauthor of a new report from the Pew Internet & American Life Project. "Use of the Internet doesn't necessarily diminish partisanship, or even zealotry. But it does expose online Americans to more points of view, and, on balance, that is a good thing." One surprise coming out of the survey -- about 20% of Americans say they actually prefer news sources that challenge their point of view, and nearly 10% are \*more\* aware of arguments that oppose their candidate than arguments in favor. (Pew Internet & American Life Project 28 Oct 2004)

### **29.4 Online & electronic voting**

Category 29.4	Online & electronic voting					
2004-01-01	electronic voting hardware operating system reliability question					
RISKS		23	11			
ELECTRONIC VOTI	IG: COMPUTER RELIABILITY ASPECTS					
tested 50 CPUs and two	describes a reliability-testing project he performed to ask about e-voting m Windows operating systems over a three-month period. His project's find ncial service application. Axtell demands, "Why is it that my financial client seem to see a need"	lings showed V	Windows to be			
Category 29.4	Online & electronic voting					
2004-01-15 online electronic Internet poll voters politicians Senate Republican Conference						
RISKS; http://atrios.blogspo ONLINE POLL RIGC	.com/2004_01_11_atrios_archive.html#107414565730750569 ING	23	13			

Contributor Keith C. Ivey writes about a case of online poll rigging by the Senate Republican Conference. When results about a poll about the capture of Saddam Hussein didn't go as expected, the recorded answers to the poll question were interchanged in secret. Ivey asks, "If politicians are willing to tamper with something as insignificant as a Web poll, how much more tempting is it to tamper with the results of a real election?"

Category 29.4 Online & electronic voting

#### 2004-01-21 electronic Internet voting criticised COTs

NewsScan

INTERNET VOTING DISPUTE

An Internet-voting program written for the Pentagon by Accenture eDemocracy Services for use by men and women serving overseas is being fiercely criticized by security experts Avi Rubin of Johns Hopkins University and retired IBM researcher Barbara Simons. Rubin says, "It's not possible to create a secure voting system with off-the-shelf PCs using Microsoft Windows and the current Internet. History has shown that when people have the opportunity to tamper with an election they do." On the other side of the issue, R. Michael Alvarez, co-director of the CalTech-MIT Voting Technology Project says: "The chance of a security threat has to be weighed against the knowledge gained and the improved voting access for those people. There's a widespread perception that Internet voting is going to happen at some time. As scientists, we'd like to lay out some kind of rational path that leads from punch cards and lever machines to that logical future." (Washington Post 21 Jan 2004)

Category 29.4 Online & electronic voting

#### 2004-01-23 electronic e-voting discourage analysis hacking fraud error quality assurance

NIPC/DHS; http://www.gcn.com/vol1\_no1/security/24681- 1.html

January 22, Government Computer News — Security analysts recommend scrapping online voting plans.

A group of security analysts who have evaluated Department of Defense (DoD) plans for an online voting pilot have recommended that the plan be scrapped because its security cannot be ensured. The analysts concluded "Internet voting presents far too many opportunities for hackers or even terrorists to interfere with fair and accurate voting." The DoD, however, said it has no intention of stopping the program. "Security was our Number One priority when we started on this concept," DoD spokesman Glenn Flood said. The Secure Electronic Registration and Voting Experiment (SERVE) is a DoD program being operated by the Federal Voting Assistance Program (FVAP) to ease absentee voting procedures for U.S. citizens living or serving overseas. A 10-member Security Peer Review Group put together by FVAP evaluated the system. A minority report was issued by four members of the group. The report said inherent flaws in proprietary software, the Internet and PCs from which votes would be cast make the process too risky to be used in a real election. Threats include insider flaws, denial-of-service attacks, spoofing attacks, and malicious code. Flood said weaknesses in the Internet infrastructure were taken into account in designing SERVE.

Category 29.4	Online & electronic voting
2004-01-30	electronic online voting citizens abroad disapproved politics
NowsScan	

NewsScan

BIPARTISAN COALITION GIVES THUMBS DOWN TO INTERNET VOTING

Politics makes for strange bedfellows, demonstrated by the pairing up of both the Republican and Democratic party organizations for U.S. citizens living abroad against the Pentagon's Federal Voting Assistance Program, which is sponsoring a \$22-million Internet voting experiment. The leaders of Republicans Abroad and Democrats Abroad have joined forces with the Association of Americans Resident Overseas, American Citizens Abroad and the Federation of American Women's Clubs Overseas in an appeal to Congress and Defense Secretary Donald Rumsfeld to stop the program now. "We've heard so much about the doubtful security of online voting, so we're concerned that we're going too fast," says the U.S. liaison for the women's clubs. "One day this might be absolutely wonderful. In the meantime, we might find ourselves with a kind of a super-2000 disaster, and people will think online voting will never be possible." The trial program is open to all overseas residents from 50 counties that have signed up with the Pentagon, but it suffered a setback last week when computer security experts released a report detailing the inherent vulnerabilities in the system what would leave it wide open to hacking. (Washington Post 30 Jan 2004)

#### 2004-02-06 electronic e-voting election Pentagon cancel security concern

NewsScan

PENTAGON CANCELS E-VOTING PLANS

Because of security concerns, the Department of Defense has canceled plans to use an electronic voting system that would have been used by Americans overseas to cast their votes next November; the system is called Secure Electronic Registration and Voting Experiment (SERVE). Deputy Defense Secretary Paul D. Wolfowitz said in a memo: "The department has decided not to use SERVE in the November 2004 elections. We made this decision in view of the inability to ensure legitimacy of votes, thereby bringing into doubt the integrity of the election results." Wolfowitz goes on to say that the system will continue to be used for testing and development purposes. Meg T. McLaughlin, president of Accenture eDemocracy Services, says the decision to continue testing the system will provide "an opportunity to demonstrate that the Internet is viable, valuable and secure enough to use for filing absentee ballots. We are confident that sending absentee ballots via the Internet is just as secure and reliable as sending them by mail." (New York Times 6 Feb 2004)

Category 29.4	Online & electronic voting
2004-02-10	electronic voting analysis flaws problems resources

http://www.nwfusion.com/newsletters/sec/2004/0209sec1.html

Securing Vote Tallies

by M. E. Kabay, PhD, CISSP Associate Professor, Computer Information Systems Norwich University, Northfield VT

Vermont has a tiny population; we have about 600,000 people in the entire state. Because of this small population, people here have many ways of becoming involved in civic affairs. Our state house in Montpelier (the smallest state capital city in the US, with 8,000 people) is open to the public, as are committee meetings. State officials such as the governor often walk about in town where ordinary citizens can chat with them in a friendly and very personal way.

I was recently invited to address the Government Operations Committee as they discussed a pending bill which would require any wholly electronic voting mechanism to be equipped with a means of producing a paper ballot that could be inspected by the voter and which would then be stored safely for official recounts. Given the importance of safeguarding the vote in our nation, I thought it might interest readers to step outside the confines of network security for a moment to consider the security implications of wholly electronic voting.

Today, there are three different forms of voting in place in use in the USA (I won't discuss remote, Internet-based voting in this column): one can mark a piece of paper by hand and have it read by people; one can mark a piece of paper by hand or machine and have it read by an optical-mark reader which tallies the results automatically; or one can use a wholly-electronic system with an input device such as a touch-sensitive screen which stores the results in a database and produces automatic tallies.

Normally, paper ballots, whether read by people or tallied by machines, are stored in sealed containers and can be opened with a court order in cases of judicially-approved recounts when election results are challenged.

In Vermont, the Secretary of State's office allows optical-mark readers to be used for elections; only one such machine is required per voting location, most of which have at most a few thousand voters registered per location. However, most locations still use manual counting of ballots under the supervision of representatives of the various political parties involved in the election.

In my testimony before the Government Operations Committee, I stressed the following points:

\* Any system of vote counting that relies on completely proprietary (secret) programs is potentially vulnerable to abuse. The underlying computer programs controlling how marks on ballots are counted in Vermont are proprietary (they are owned by Diebold Corporation), but the technicians who prepare the configuration tables relating a position on a ballot to a particular name work for an independent consultancy in Massachusetts and their configuration tables are open for inspection.

\* Every optical tabulator is tested to see if it reads ballots correctly before the election begins.

\* Passing a law that allows the Secretary of State to order a random check on the accuracy of machine tallies in any voting district will help prevent systematic fraud. The tallies in a manual recount must match the machine tallies to within an acceptable error rate (to allow for the inherent difference between machine tallies and human counting methods: machine reject incorrectly-marked ballots whereas people can agree on the intention of the voter).

\* Wholly-computer-based voting systems have far more vulnerabilities to tampering than optical-mark sensors. We know that even companies such as Microsoft have allowed Easter Eggs (unauthorized, undocumented code such as flight simulators) to escape quality assurance and be delivered to customers in software such as MS-Excel. We know that microprocessors have been tampered with to cheat clients and evade testing (e.g., gas pump meters in the Los Angeles district were designed to overcharge customers by 10% -- unless they noticed one- or five-gallon deliveries, which were the volumes typically used by inspectors when checking accuracy). We know that production code has been profoundly flawed for years without being caught (e.g., the Colorado lottery's not-very-random-number generator that produced only numbers from zero to eight but never any nines). We know that data stored in databases without careful attention to chained cryptographic checksums involving timestamps, sequence numbers and the previous record's checksum can be modified to misrepresent election results.

\* For all these reasons, we should resist the use of wholly-computerized voting machines until there is software that is entirely open to inspection.

\* Any wholly-electronic voting machine should be required to produce a paper ballot showing the voter's choices for inspection by that voter (only). The voter should then be required to place the ballot in a ballot box for use in judicial recounts and random testing of the accuracy of the computerized voting system.

\* \* \*

#### For further reading:

Background paper on all aspects of electronic voting < http://lorrie.cranor.org/voting/hotlist.html > White Paper on the use of receipts in voting < http://www.vreceipt.com/article.pdf > Dangers of proprietary code in voting machines < http://www.blackboxvoting.org >

See also several articles and press releases about electronic voting on the Electronic Frontier Foundation Web site at < http://www.eff.org > and reports on the activist Web site < http://www.verifiedvoting.org >.

<i>Category 29.4</i> 2004-02-15	Online & electronic voting e-voting machine errors election invalidated		
RISKS		23	19
MISSISSIPPI VOIDS NOVEMBER 2003 E-VOTE ELECTION FOR ERRORS			

Rebecca Mercuri contributed a report on the failure of WINnVote touchscreen voting machines in Hinds County, Mississippi in the November 2003 election. "Poll workers had trouble starting the machines, some of the machines overheated and had to be taken out of service, poll workers were scrambling to find enough paper ballots, and many voters left with polls without voting because of the long delays." As a result of the SNAFU, the Mississippi Ssenate ordered a new election.

Category 29.4	Online & electronic voting		
2004-02-25	e-voting physical security tampering fraud hacking		
RISKS		23	20
PHYSICAL SECUR	TTY OF ELECTRONIC VOTING TERMINALS		

Tobin Fricke reported in RISKS on sloppy security for e-voting equipment: "A cart of Diebold electronic voting machines was delivered today to the common room of this Berkeley, CA boarding house, which will be a polling place on Tuesday's primary election. The machines are on a cart which is wrapped in plastic wrap (the same as the stuff we use in the kitchen). A few cable locks (bicycle locks, it seems) provide the appearance of physical security, but they aren't threaded through each machine. Moreover, someone fiddling with the cable locks, I am told, announced after less than a minute of fiddling that he had found the three-digit combination to be the same small integer repeated three times.

One wonders whether paper ballots would be handled differently, how the terminals are stored between elections, what checks are done for tampering before the use of the terminals, and what physical security features are built into them."

Category 29.4 Online & electronic voting

2004-03-02 electronic e-voting touch screen voting machine issues political

NewsScan

TOUCHY (AND UNCLEAR) SUBJECT

Supporters of the new touch-screen voting machines promise paperless elections cheaper and faster to administer, but there are plenty of skeptics. David Jefferson, a computer scientist at the Lawrence Livermore National Laboratory, warns: "Once a ballot is cast, you can't pull it back out. After the fact, you cannot recover from problems. It's not like a financial system, where you can take reasonable risks; in voting, you just can't." MIT computer science professor Ted Selker, more optimistic about the machines, says: "There are things that are scary that don't happen. And the versions of the software have been such that somebody with nefarious goals would be as confused as the rest of us if they tried." CalTech political scientist R. Michael Alvarez agrees with Selker, but adds: "The issue of voting systems has gotten very politicized in the last year. The overriding issue now is that there's an enormous amount of uncertainty election administrators have about what technological change is happening and what's going to be permitted under the law, and it's not entirely clear that we're going to have the technology to meet the requirements that have been put out there." (Los Angeles Times 2 Mar 2004)

Category 29.4	Online & electronic voting		
2004-03-02	e-voting failures bootup delays disenfranchisement		
RISKS		23	25
E-VOTING FAILU	JRES IN CALIFORNIA		
		A 11 C - 1	

A posting in RISKS 23.25 reported a number of e-voting failures in California for local elections. All of the reported problems involved systems refusing to boot. Voters were turned away, sometimes several times, and told to try again later in the day. Some of these would find it difficult to get back to their home precincts after work in time to vote.

Category 29.4	Online & electronic voting
2004-03-03	electronic online e-voting glitches elections frozen screens malfunctions

NewsScan

ELECTRONIC VOTING SUFFERS GLITCHES

Voters in California, Georgia and Maryland reported problems with their attempts to cast electronic ballots, citing a frustrating mix of frozen screens, encoder problems and other malfunctions that caused delays of up to two hours and forced some voters to travel to other polling sites to cast old-fashioned paper ballots. Election officials blamed improperly trained poll workers, but critics say Tuesday's experience is just a harbinger of worse things to come next fall, when at least 50 million voters — almost half of the expected voter turnout — will use touch-screen voting systems. "Unless Congress deals with this problem immediately by requiring voting machines to produce a paper record voters can verify, we're going to have more of these occurrences each time we have an election, including this November," says New Jersey Rep. Rush Holt. "The only question is, how long it will take before voters lose faith in a system that they thought was being fixed?" (AP 3 Mar 2004)

Category 29.4 Online &	electronic voting
------------------------	-------------------

#### 2004-03-30 electronic e-voting Pentagon test end

NewsScan

PENTAGON ENDS TEST OF INTERNET VOTING

The U.S. Department of Defense has decided to terminate its \$22 million pilot project designed to test Internet voting for 100,000 American military personnel and civilians living overseas. Because of concerns about the security of online voting, the department had already decided not to allow Internet ballots to be counted in the presidential election, and has now decided to scrap the whole project — at least for the discernible future. A Pentagon spokesman says: "It's not that it's never going to go in test mode. It's that right now we're not going to do it. We have to step back and look at everything that we've done for two or three years in this thing. But right now we're not going forward." (AP/Washington Post 30 Mar 2004)

Category 29.4 Online & electronic voting

#### 2004-04-13 electronic voting

http://www.dissidentvoice.org/April2004/Landes0413.htm

As the battle over voting machines rages across the country, the U.S. Commission on Civil Rights met on 9 Apr 2004, to examine the "Integrity, Security and Accessibility in the Nation's Readiness to Vote." Two scientists and four representatives of civil rights organizations were invited to brief the Commission.

But, before the panelists had a chance to share their views, three Republican commissioners and one (notably conservative) Independent commissioner walked out, ostensibly over a personnel dispute. But, others are not so sure.

It appears that voting technology is a topic that the Republican leadership wants to tightly control. It is without doubt that Republicans own most of the companies that manufacture, sell, and service voting machines. And President Bush and the Republican Congress appear determined to control and limit oversight of the elections industry. The Bush Administration has stacked the Election Assistance Commission with supporters of paperless voting technology, while the National Institute of Standards and Technology's (NIST) got walloped with a \$22 million budget cut in fiscal 2004, which means that NIST will have to cut back substantially on its cyber security work, as well as completely stop all work on voting technology for the Help America Vote Act.

2004-04-22	India e-voting general elections largest democracy save trees
Category 29.4	Online & electronic voting

NewsScan

INDIA IMPLEMENTS E-VOTING

For decades, millions of illiterate Indians voted by pressing their thumbprints on ballot cards. This year, they'll just press a button -- and so will everyone else. India's general elections, which began Tuesday, are set to make the world's largest democracy also the world's largest user of computerized voting machines. This year, in a staggered vote that runs through May 10, India's 660 million registered voters will be able to exercise their franchise on one of approximately 1 million computerized voting machines in an electronic, ballot-less election. The change in India is having a deep impact on politics. Supporters say it's also good for the environment in a country trying to save its vanishing forests. More than 8,000 tons of paper, made from approximately 16 million trees, has been used to print ballots for past federal elections. (The Australian 22 Apr 2004)

Category 29.4 Online & electronic voting

2004-04-22 e-voting electronic paper backups battery failure Marlyland lawsuit lose

NewsScan

MD. GROUP DEMANDS PAPER BACKUP FOR E-VOTES

A voter advocacy group in Maryland is suing that state's Board of Elections to prevent the use of touch-screen voting machines until a paper record is installed as auditable backup for the system. At present, the state's Diebold voting machines are not set up to produce a paper record of each individual vote. Linda H. Lamone, the state elections administrator, says that paper records are unnecessary because the Diebold system is equipped to preserve votes in its memory: "It's stored in two different locations. If we have battery failure, it still doesn't lose votes." She also said: "It's going to be next to impossible for anyone to gain access to manipulate the election. If anyone tries it, we're going to put them in jail." (Washington Post 22 Apr 2004)

Category 29.4 Online & electronic voting

#### 2004-04-22 e-voting paperless Diebold touch-screen security errors

NewsScan

CALIFORNIA PANEL NIXES DIEBOLD VOTING MACHINES

California's Voting Systems and Procedures Panel has recommended discontinuing the use of 15,000 its Diebold touch-screen voting machines, saying that the systems had malfunctioned in the state's March primary election in March and caused many voters in San Diego County to be turned away. (AP/USA Today 22 Apr 2004)

Category 29.4 Online & electronic voting

#### 2004-04-24 electronic e-voting legislators wary Diebold concern

DHS IAIP Daily;

http://www.washingtonpost.com/wp- dyn/articles/A38997- 2004Apr 24.html

April 24, Associated Press — Legislators wary of electronic voting.

Computer scientists have long criticized touchscreen voting machines as not being much more reliable than home computers, which can crash, malfunction and fall prey to hackers and viruses. Now, a series of failures in primaries across the nation has shaken confidence in the technology installed at thousands of precincts. At least 20 states have introduced legislation requiring a paper record of every vote cast. On Thursday, April 22, a California panel unanimously recommended banning a Diebold Inc. paperless touchscreen model. Secretary of State Kevin Shelley, who said Diebold glitches "jeopardized the outcome" of the March 2 primary, has until April 30 to decide whether to decertify Diebold and possibly other touchscreen terminals in California. The bipartisan U.S. Election Assistance Commission, formed in January to develop technical standards for electronic voting, will conduct a May 5 public hearing in Washington, DC. Computer scientists say paperless systems made by Sequoia Voting Systems Inc. and other competitors also expose elections to malicious attack, software glitches and mechanical errors that could delete or alter millions of ballots.

## Category 29.4 Online & electronic voting 2004-04-29 Diebold electronic paperless voting machines vulnerabilities hacking perversion distortion election

http://www.nytimes.com/2004/05/03/technology/03vote.html?th=&pagewanted =print&position=

Professor Aviel Rubin, Technical Director of the Information Security Institute of Johns Hopkins University, demonstrated the vulnerability of paperless electronic voting systems to hacking in a classroom demonstration in April. As John Schwartz of the New York Times wrote, "The fix was in, and it was devilishly hard to detect. Software within electronic voting machines had been corrupted with malicious code squirreled away in images on the touch screen. When activated with a specific series of voting choices, the rogue program would tip the results of a precinct toward a certain candidate. Then the program would disappear without a trace."

Professor Rubin published an analysis of 49,000 lines of the bold voting machine code in July 2003. the security implications were grim, as he and his colleagues wrote: "Our analysis shows that this voting system is far below even the most minimal security standards applicable in other contexts. We conclude that, as a society, we must carefully consider the risks inherent in electronic voting, as it places our very democracy at risk." in a report on his experience as an election scrutineer, he wrote, "I started realizing that some of the attacks described in our initial paper were actually quite unrealistic, at least in a precinct with judges who worked as hard as ours did and who were as vigilant. At the same time, I found that I had underestimated some of the threats before.... I continue to believe that the Diebold voting machines represent a huge threat to our democracy."

## Category 29.4 Online & electronic voting 2004-05-06 Diebold electronic paperless voting machines vulnerabilities hacking perversion distortion election

#### http://www.computerworld.com/printthis/2004/0,4814,92950,00.html

Voting-machine vendors sneered at the analysis of security vulnerabilities presented in testimony before the U.S. Election Assistance Commission in early May 2004. Officials received scientific reports of simple introduction of Trojan horse software into the machines to distort election results, the impossibility of verifying accuracy of results without a voter-verified paper ballot for audit purposes, and the use of inadequate encryption for transmission of data (including a single hardwired key for all the voting machines). The representatives of the voting machines dismissed the objections as theoretical and unrealistic but never addressed the fundamental problem: a voter cannot know whether his or her vote has been registered correctly by the machines if there is no independent mechanism of validation.

Category 29.4	Online & electronic voting
2004-05-06	Diebold voting machines security problems lawsuits

#### NYT Circuits

David Pogue of the New York Times wrote a blistering editorial criticizing Diebold and other electronic-voting machine manufacturers. He wrote,

>Remember how, a few months back, I expressed my horror that Diebold's touch-screen voting machines, which one in five Americans will use in this fall's elections, were failing every security test? Its technicians make changes to the machines' software AFTER inspection by local election boards. The machines' software is not made available for public inspection — an unacceptable situation in what's supposed to be a democracy. And incredibly, these machines produce no paper record of the votes.

They're also buggy. During California's presidential primary in March, machines in more than half of San Diego County's precincts malfunctioned.

I'm happy to report that the nation is finally waking up. Many states, as well as Federal lawmakers, are considering legislation that requires voting machines to leave a paper trail. Better yet, California Secretary of State Kevin Shelley had the guts to ban or decertify tens of thousands of Diebold machines across California. He's even considering filing criminal or civil charges against the company.

My guess is that if the defiant, unhelpful Diebold doesn't start showing some humility, fixing its work and letting the public see what it's doing under the hood, California will be only the first state of many to get wise.<

#### Category 29.4 Online & electronic voting

#### 2004-05-12 e-voting Diebold fund-raising politics marketing mistake error

http://www.nytimes.com/2004/05/12/politics/campaign/12vote.html

Walden W. O'Dell, the chairman and chief executive of Diebold Inc., said on Monday [10 May 2004] that it had been a "huge mistake" for him, as the head of a voting machine company, to express support for President Bush's re-election in a fund-raising letter last year. Mr. O'Dell also said the company was working to address computer security problems and build voter confidence in its wares.

Category 29.4	Online & electronic voting
2004-05-24	e-voting electronic voting concerns Virginia study

#### DHS IAIP Daily;

http://www.washingtonpost.com/wp- dyn/articles/A51595- 2004May 24.html

May 24, Washington Post — E- voting woes prompt Virginia study.

Virginia General Assembly leaders say they will soon appoint members of a new commission that will study the security and reliability of electronic voting machines, a response to growing concerns that new- generation voting technology may be riddled with problems. Commission members could be announced as soon as this week, though the final list may not be named until the end of June. The commission will be composed of six members of the General Assembly and five private citizens. They will study how voting equipment is certified and tested and how the equipment should be handled before, during and after it is used. The panel ultimately could propose a statewide system for verifying electronic voting machine accuracy, according to lawmakers and other officials involved in the commission's creation. Lawmakers, academic experts and citizen- activists across the country are urging changes in how the machines work, proposing that electronic voting machines produce paper receipts for each vote. Another proposal is to require the software that powers new voting machines to meet certain standards set by public officials. California and Ohio currently require that electronic voting machines have verifiable paper trails by 2006.

Category 29.4 Online & electronic voting

#### 2004-06-08 electronic voting e-voting research Election Assistance Commission

NewsScan

E-VOTING OVERSEER WANTS 'MORE RESEARCH' ON PAPER BACKUP BALLOTS

DeForest B. Soaries, the head of the federal Election Assistance Commission, says he wants election officials to be able to analyze software source code in the electronic systems they purchase. Some vendors have resisted providing source code, on the ground that it is proprietary information. As for requiring that the systems produce paper copies of votes cast electronically, Soaries is undecided: "If there was unanimity among scholars and scientists on the paper issue it would be a more compelling case. All of the research, all of the testimony we've received, all the writings that I've read argue for more research." (AP/Los Angeles Times 8 Jun 2004)

Category 29.4 Online & electronic voting

#### 2004-06-14 electronic e-voting paperless League of Women Voters

NewsScan

LEAGUE OF WOMEN VOTERS SAYS NO TO PAPERLESS VOTING SYSTEMS

The League of Women Voters has withdrawn its support of electronic voting machines that can't produce auditable paper backup copies of individual ballots. Computer scientist Barbara Simmons, a member of the League as well as a past president of the Association for Computing Machinery (ACM), said: "My initial reaction is incredible joy and relief. This issue was threatening to split the League apart... The league now has a position that I feel very comfortable supporting." (AP/San Jose Mercury News 14 Jun 2004)

2004-07-07	electronic e-voting concern fear threat California Americans with Disabilities
Category 29.4	Online & electronic voting

NewsScan

E-VOTING CONCERNS

California's Secretary of State has won a victory in federal court and new agreements from counties with touch-screen machines to make extra security arrangements. U.S. District Judge Florence-Marie Cooper denied requests by disability rights activists and four California counties to

overturn the Secretary's conditional April 30 ban on touch screens for the November election. In the suit, disability groups argued that banning electronic voting will deny hundreds of thousands of people the right to vote in private, but the judge ruled the Americans With Disabilities Act requires only that disabled voters be given the opportunity to vote. (Bloomberg News/San Jose Mercury News 7 Jul 2004)

Category 29.4	Online & electronic voting
2004-07-12	Diebold electronic e-voting systems manufacturer whistleblower lawsuit fraud California

NewsScan

"WHISTLEBLOWER" LAWSSUIT FILED AGAINST DIEBOLD

Opponents of electronic voting are suing Diebold Inc. under a California whistleblower law, accusing Diebold of defrauding the state by providing shoddy balloting equipment that exposed California elections to vandals and to software bugs. The individuals who filed the suit are Jim

March, a programmer, and Bev Harris, an activist. Under the whistleblower statute, the two could collect up to 30% of any reimbursement. March says: "This is about money now -- a case of the capitalist system at work. The laws on voting products and processes are unfortunately unclear. But the law on defrauding the government is really, really clear. Going after the money trail is cleaner than going after proper procedures." But some critics of Diebold are equally critical of March and Harris. One of them says, "I would like to see people support a real solution rather than just try to cash in. There are a lot of people who could be a tremendous asset, but they're grandstanding and reveling in the expose." (San Jose Mercury News 12 Jul 2004)

```
Category 29.4 Online & electronic voting
```

#### 2004-07-19 Ohio voting machine electronic Diebold security problem

NewsScan

OHIO QUESTIONS VOTING MACHINE USE

Ohio Secretary of State Kenneth Blackwell has blocked three counties in that state from using Diebold electronic voting machines in November because the systems have shown security problems. Some of the state's 88 counties already were using electronic voting machines, and the decision does not affect them. A Diebold executive says, "We are anxious to learn the areas where the consultant believes additional work is needed." (AP/San Jose Mercury News 19 Jul 2004)

Category 29.4 Online & electronic voting

2004-08-05 electronic e-voting system touchscreen South Carolina election attorney general

NewsScan

APPROVAL FOR TOUCHSCREEN VOTING SYSTEM

Ruling that the state's new touch-screen voting machines meet federal requirements, the South Carolina attorney general has rejected a request from the South Carolina Progressive Network (SCPN) to stop the State Election Commission from buying the machines. The SCPN's objections to the machines are that they do not provide proof on paper that the vote was cast the way the voter intended, but the attorney general ruled that the state's new machines give voters a chance to review and make changes to the ballots before finalizing their votes. (AP/USA Today 5 Aug 2004)

## Category 29.4 Online & electronic voting 2004-08-05 Hack the Vote challenge Defcon 12 Rebecca Mercuri abandon e-voting systems 2004 elections

DHS IAIP Daily; http://www.pcworld.com/news/article/0,aid,117261,00.asp

August 05, PC World — Can you hack the vote?

E- voting technology expert Rebecca Mercuri, a Harvard research fellow, has issued a "Hack the Vote" challenge, trying to illustrate what she calls their unreliability and vulnerability. She unveiled the so- called Mercuri Challenge at the recent Black Hat Briefings and Defcon 12 security conferences. Mercuri suggests electronic voting machines be hacked during their preelection testing, so officials will abandon them before an actual election. As part of her challenge, Mercuri is calling on e- voting system vendors VoteHere and Advanced Voting Solutions to supply any challengers "full specifications" of their voting system for review. The first person to undetectably change vote tallies can claim \$10,000 from a separate challenge. Tom Mereckis, head of marketing for VoteHere, says VoteHere makes full specifications of its voting systems available to anyone. Conversely, the president of Advanced Voting Solutions says he has no intention of ever releasing the proprietary workings of its voting systems.

Category 29.4 Online & electronic voting

#### 2004-08-06 electronic e-voting Defcon 12 security experts skeptical

DHS IAIP Daily; http://www.computerworld.com/securitytopics/security/story/0,10801,95094,00.html

August 06, Computerworld — Public, security experts' e- voting views differ sharply.

Security experts are substantially more skeptical about e- voting than the public, but their greatest worry is system and programming errors, not malicious hacker attacks, according to a survey released last week by the Ponemon Institute. The study, conducted in July and early August, aimed to measure public opinion about electronic voting systems and then compare the results with those of security experts- - both IT pros and hackers. The Tucson, AZ- based institute collected 2,933 usable responses nationwide from the public, both online and by postal mail, and surveyed 100 attendees at the Black Hat and Defcon hacking/security conferences. Six out of 10 Black Hat/Defcon attendees had an unfavorable view of e- voting, while only 17% of the public did. Twenty percent of the experts cited system and programming errors as their top concern, followed by attempts to influence the outcome of an election. A potential breach of security by hackers and cybercriminals ranked third as a potential e- voting worry among the Black Hat/Defcon attendees. Among the public, the top worry was a decline in voter turnout because of fear or distrust of e- voting systems, followed by human errors and privacy violations.

Category 29.4 Online & electronic voting

#### 2004-08-10 electronic e-voting petition Maryland Diebold security question

DHS IAIP Daily;

http://www.computerworld.com/governmenttopics/government/policy/story/0,10801,95162,00.html

August 10, IDG News Service — Maryland voters file petition against e- voting system.

Eight Maryland voters have asked an appeals court to force the Maryland State Board of Elections (SBE) to address alleged security risks in a Diebold electronic voting machine system and provide a voter- verified paper trail during elections. The plaintiffs, some representing advocacy group TrueVoteMD.org, accuse the SBE of ignoring scientific and government studies that question the security of the Diebold e- voting machines and of ignoring a Maryland legislative requirement to include a voter- verified paper trail with an e- voting system. Such a paper trail would allow voters to check their electronic votes against paper printouts, which can then be used to audit the election results, said Linda Schade, director and cofounder of TrueVoteMD.org.

## Category 29.4 Online & electronic voting 2004-08-17 voting data database Australia safe integrity authenticity possession privacy voter information

NewsScan

VOTER DATA 'SALE' IN AUSTRALIA

The Australian Electoral Commission will investigate whether the Liberal Party has on-sold to its federal and state candidates political databases containing private information about voters, in breach of federal electoral laws. Former ministerial staffers have told The Australian the Liberal Party secretariat has offered discounts to ensure candidates buy the Feedback database, which contains personal information about their constituents based on Australian Electoral Roll electronic data. AEC spokesman Brien Hallett said the law prohibited the use of protected electoral roll data being used for "commercial purposes," but that definition would need to be tested by a court. (The Australian 17 Aug 2004) Rec'd from John Lamp, Deakin U.

## Category 29.4 Online & electronic voting 2004-08-23 electronic e-voting machine certification criticism testers hardware software Federal Election Commission

DHS IAIP Daily;

http://www.cnn.com/2004/TECH/biztech/08/23/evoting.labs.ap/index.html

August 23, Associated Press — E- vote machine certification criticized.

Although up to 50 million Americans are expected to vote on touchscreen voting machines on November 2, federal regulators have virtually no oversight over testing of the technology and critics allege that the three companies that certify the nation's voting technologies operate in secrecy, and refuse to discuss flaws in the ATM- like machines. Federal regulations specify that every voting system used must be validated by a tester. Yet it has taken more than a year to gain approval for some election software and hardware, leading some states to either do their own testing or order uncertified equipment. The election directors' voting systems board chairman, former New York State elections director Thomas Wilkey, said the testers' secrecy stems from the Federal Election Commission's refusal to take the lead in choosing them and the government's unwillingness to pay for it, leaving election officials no choice but to find technology companies willing to pay. A 2002 law, the Help America Vote Act, created a four- member, bipartisan committee, headed by U.S. Election Assistance Commission chairman DeForest Soaries Jr., to oversee a change to easier and more secure voting. Soaries said there should be more testers but the three firms, CIBER and Wyle Laboratories in Huntsville, AL, and SysTest Labs in Denver, CO, are "doing a fine job with what they have to work with."

Category 29.4 Online & electronic voting

#### 2004-08-25 California electronic e-voting approval

DHS IAIP Daily; http://www.theregister.co.uk/2004/08/25/evoting\_california/

August 25, The Register — California approves e- voting.

California will allow voting at electronic voting machines in November in 11 of the state's counties. Kevin Shelley, California's secretary of state, said that the counties had improved the security of their voting machines so that they now comply with all conditions required for state certification. Four counties that remain unapproved are those using the Diebold AcuVote- TSx Voting System voting machines. Shelley decertified the machines in April after problems with the March elections. California has invested more than \$139 million on electronic touch screen technology, and during the March presidential primary vote 42 percent of the state's voters could have had access to 42,714 electronic voting machines.

### Category29.4Online & electronic voting2004-08-30Missouri electronic e-mail voting security concern military overseas ballots

DHS IAIP Daily;

http://story.news.yahoo.com/news?tmpl=story&ncid=1212&e=4&u= /ap/20040828/ap\_on\_hi\_te/voting\_by\_e\_mail&sid=95573501

August 30, Associated Press — E- mail voting prompts security concerns.

Missouri will allow members of the military stationed overseas to return absentee ballots via e- mail, raising concerns from Internet security experts about fraud and ballot secrecy. State and federal officials insist safeguards, such as signature verification and tracking numbers, are in place to protect the ballots from tampering, duplication or other forms of fraud. However, some critics warn that e- mail is fundamentally insecure. "E- mail is subject to all kinds of tampering," said Bruce Schneier, co- founder of Mountain View, CA- based Counterpane Internet Security Inc. Missouri appears to be the first state using the e- mail option, but other states also could adopt it. About half of states permit electronic transmission of voted ballots, generally by fax, and could follow Missouri's lead, according to the Pentagon's Federal Voting Assistance Program. Ballot secrecy is not available with e- mail and sending such a message is akin to sending a postcard, with its content easily viewable in transit using widely available software. Military personnel are told upfront that their e- mailed ballots won't be secret and that they can mail them in instead. Because of security concerns, the Pentagon earlier this year canceled an Internet voting plan that would have allowed as many as 100,000 military and overseas citizens from seven states to cast votes in November through a Web browser.

Category 29.4 Online & electronic voting

2004-09-01 touch-screen electronic e-voting judge ruling Circuit Court Maryland OK

NewsScan

MARYLAND JUDGE OKAYS TOUCH-SCREEN VOTING

Rejecting a challenge to the state's touch-screen voting machines, a Circuit Court judge in Maryland suggests that the machines are more accurate than the paper ballots the plaintiffs are seeking to make optional for the November elections, and notes that election officials have "taken all

reasonable steps to protect the integrity of the voting process." The lead plaintiff's response is: "I am very disappointed that Maryland voters will be forced to vote on machines that we believe are illegal under Maryland law and that are clearly very insecure." In his ruling the judge wrote: "No

system is infallible. No machine is infallible. All experts agree systems such as these are much more secure and less vulnerable than the paper ballot" -- or the optical scan machines used in most Maryland jurisdictions in the last presidential election. (Washington Post 1 Sep 2004)

Category 29.4 Online & electronic voting

### 2004-09-07 electronic e-voting paper trail audit Nevada elections 2004 example US states legislation

DHS IAIP Daily; http://securityfocus.com/news/9461

September 07, The Associated Press — Nevadans to become first to use touch- screen voting that produces a paper trail.

In what could become a model for other states, Nevada voters on Tuesday, September 7, became the first in the nation to cast ballots in a statewide election on computers that printed paper records of electronic ballots. Nevada's \$9.3 million voting system includes more than 2,600 computers and printers deployed in every county. California, Washington and Illinois recently passed laws requiring a paper trail for electronic ballots, and at least 20 others are considering similar legislation. The system aims to address concerns that paperless touchscreen votes cannot be properly audited or recounted. As many as 50 million Americans will cast ballots in the November presidential election on electronic machines that do not produce a paper receipt of the vote.

Category 29.4	Online & electronic voting
2004-09-08	electronic e-voting Nevada security audit concern Sequoia touchscreen

NewsScan

E-VOTING IN NEVADA

Nevada voters have become the first in the nation to cast ballots in a statewide election using computers that produced printed paper records of electronic ballots. "Knock on wood, so far things have been working flawlessly," said Secretary of State Dean Heller. Nevada's \$9.3 million voting system includes more than 2,600 computers and printers deployed in every county. The system, developed by California-based Sequoia Voting Systems, aims to address concerns that paperless touchscreen votes cannot be properly audited or recounted. "From what I've seen, voters seem to enjoy the experience," says DeForest B. Soaries Jr., chairman of the U.S. Election Assistance Commission. "There hasn't been frustration or confusion."(AP/USA Today 8 Sep 2004)

Category 29.4 Online	&	electronic voting
----------------------	---	-------------------

2004-09-13 electronic e-voting Nevada primary California observe accurate recording

NewsScan

E-VOTING IN NEVADA

Nevada \$9.3 million voting system worked well in last week's primary. California official Marc Carrel, who observed the election, says, "They were incredibly organized. I think California could pull off a similar election if we had adequate training and education programs for poll workers and

voters." Printers attached to the systems offer assurances that elections can be fully audited, and a spokesman for Sen. Dianne Feinstein says, "The Nevada election demonstrates that you can have efficient electronic voting machines yet at the same time have a paper trail so voters can be assured

they've voted accurately and their vote is being recorded accurately." But Georgia elections director Kathy Rogers warns that the printers could have unintended consequences, allowing unethical poll workers to determine how individuals voted: "We seem to have traded a secret ballot for this piece of

paper." (AP/USA Today 13 Sep 2004)

Category 29.4 Online & electronic voting

#### 2004-10-18 survey online ratings reliability trustworthiness accuracy authenticity

NewsScan; http://www.pewinternet.org/

ONLINE RATING RANKS HIGH WITH ONE IN FOUR INTERNET USERS

Twenty-six percent of adult Internet users in the U.S. have participated in "reputation systems" -- those online rating systems used by Amazon, eBay and others to assist other users in deciding whether a product or service is trustworthy, worthwhile or enjoyable. Men are slightly more likely to offer their opinions than women (29% vs. 22%) and Generation Yers are more likely than Baby Boomers to have posted a rating (30% vs. 23%). In addition, those from wealthier households (income above \$75,000) are more likely to participate in rating than those who live in households with an income below \$30,000. The findings provide evidence that the trend toward using the Internet for two-way communication among online communities is increasing. "Internet users see these systems as a way to help them figure out what information and people they can trust online," says Paul Hitlin, a research associate at the Pew Internet Project, which conducted the study. "People also see the Internet as a place where they can voice their own opinions. Online they can recommend a CD, warn about a dishonest salesperson, or even defend their high school history teacher."

## Category 29.4 Online & electronic voting 2004-10-27 e-voting Diebold Election Systems Software Hart InterCivic Sequoia proprietary source code audit reliability trustworthiness quality assurance open-soure

NewsScan; http://apnews.excite.com/article/20041027/D85VOSTG1.html E-VOTING COMPANIES DIVULGE \*SOME\* SOFTWARE CODE

Electronic voting equipment makers Diebold Election Systems, Election Systems & Software, Hart InterCivic and Sequoia Voting Systems have agreed to submit millions of lines of software code to the National Software Reference Library, but have refused to include their most valuable data -- their proprietary source code. They also say they might not provide the library with copies of software patches and updates. The companies acted at the request of the U.S. Election Assistance Commission, whose chairman noted that although the data submitted was far from complete, he hoped the companies' ongoing submissions would eventually result in making election software more transparent. A number of scientists have called for "open source" voting software that could be independently verified, but many computer security experts remain pessimistic because no technology exists today that would allow an election official who suspects fraud to check software code on a voting machine and compare with the code stored in the library. Avi Rubin, technical director of the Johns Hopkins Information Security Institute, called the code-sharing program "meaningless." (AP 27 Oct 2004)

#### Category 29.4 Online & electronic voting

### 2004-11-03 touchscreen e-voting Sequoia Voting Systems glitches problems bugs failures flaws problems denial-of-service DoS availability

NewsScan;

http://www.cnn.com/2004/TECH/11/03/electronic.voting.ap/index.html

#### TOUCHSCREEN VOTING SPAWNS GLITCHES

U.S. voters across the country reported some 1,100 problems with e-voting machines, bearing out scientists' concerns that touchscreen machines are prone to tampering and unreliable unless they're equipped to print out paper records for recounts. Some problems were blamed on factors as mundane as power outages and incompetent poll workers, but there were a number of voters in six states -- especially Democrats in Florida -- who said that although they voted for John Kerry, when the computer asked them to verify their choice, it indicated that they had voted for President Bush. One voter in Clearwater reported that it took her about 10 tries and a quick touchscreen clean-up with a wet-wipe towel before she could successfully select Kerry. A spokesperson for Sequoia Voting Systems said the machines' monitors may need to be recalibrated periodically to ensure the touchscreen is sensitive enough to record users' votes. (AP/CNN.com 3 Nov 2004)

### 29.6 Flash crowds, social e-links

## Category29.6Flash crowds, social e-links2004-04-20critical thinking disintermediation flash crowds psyops information warfare<br/>homeland security

Network World Fusion

http://www.nwfusion.com/newsletters/sec/2004/0419sec1.html & http://www.nwfusion.com/newsletters/sec/2004/0419sec2.html

Critical Thinking and Disintermediation

by M. E. Kabay, PhD, CISSP Associate Professor, Computer Information Systems Norwich University, Northfield VT

One of the battlespaces of information warfare is the cognitive domain: knowledge, perception, attitudes and mood. For example, military campaigns have long used propaganda and misinformation to influence both the military decisions of the enemy and to discourage soldiers and civilians. In the Second World War, for example, the Nazis used radio broadcasts into Britain to spread false information about the progress of the war; conversely, the Allies broadcast to the peoples of the Axis powers to blame the governments, but not the population, for the war, thus attempting to drive a wedge between civilians and their regimes. In more recent years, there was a scandal in the USA in October 1986 about a reputed disinformation campaign during the Reagan administration in which government officials were accused of misleading the press to convey false information to Libyan dictator Qaddafi about an imminent attack. And of course currently there's a major division in the USA between those who argue that the administration deliberately misled the American people into a pre-emptive attack on Iraq versus those who suggest that the decision was based on incorrect information (or, for that matter, was correct despite the failure to find corroborative evidence of weapons of mass destruction).

Prof. Daniel Kuehl, PhD, is the distinguished Professor and Director of the Information Strategies Concentration Program at the Information Resources Management College of National Defense University in Fort McNair, Washington DC. A frequent contributor to scholarly analysis of information warfare, Dr Kuehl was the keynote speaker on Thursday the 11th of March 2004 at the 17th Annual Meeting of the Federal Information Systems Security Educators' Association at the University of Maryland University College. After his lecture, we got into a discussion about the information warfare implications of a couple of trends in modern society: disintermediation and the lack of critical thinking in the population at large.

Disintermediation in general is defined by the Webopedia as "Removing the middleman. The term is a popular buzzword used to describe many Internet -based businesses that use the World Wide Web to sell products directly to customers rather than going through traditional retail channels. By eliminating the middlemen, companies can sell their products cheaper and faster. Many people believe that the Internet will revolutionize the way products are bought and sold, and disintermediation is the driving force behind this revolution."

Disintermediation in the distribution of news is the phenomenon of reducing gate-keepers in the flow of information from provider to user. For example, Matt Drudge is free to spread unsubstantiated rumors to a huge audience without having to bother with the fact-checking that is customary in responsible news media such as reputable newspapers or magazines and some television or radio programs.

Critical thinking is the ability to analyze information skeptically rather than gullibly. For example, people who open unexpected attachments in e-mail from friends are failing to distinguish among different targets of trust:

\* Trust in the authenticity of the FROM line of an e-mail message (which may not, in fact, correctly identify the source);

\* Trust in the technical competence of the sender to evaluate the quality of the attachment (which may not, in fact, correlate with how loveable and friendly Aunt Gladys is);

\* Trust in the authenticity of the labeling of the attachment (which may not, in fact, really be a document at all but may be an executable);

\* Trust in the description and safety of an attachment (which may not, in fact, be a screen saver with frogs).

Now couple disintermediation with a lack of critical thinking. Consider the likely effects of a concerted campaign to, say, spread a number of rumors about major publicly-traded companies. We know that pump 'n' dump schemes have successfully manipulated stock values to the benefit of criminals; why not expect terrorists to apply the same techniques to manipulating the entire stock market? If people are willing to believe and act upon stock tips e-mailed to them by total strangers using spam (even though tiny print clearly states that the junk mailer has been paid to distribute the information), why wouldn't uncritical thinkers cheerfully act on "advice" spread by enemies of the nation?

Similarly, the phenomenon of flash crowds worries me: training people to assemble on command in large numbers at, say, shoe stores, piano showrooms or restaurants for no good reason other than the fun of being part of a huge crowd is a perfect setup

#### IYIR 2004

for creating an army of willing, mindless drones who will congregate on command at the site of a terrorist attack or at places where their presence will interfere with response to criminal or terrorist activities. Want to rob a bank in peace and quiet? Set up a conflict between two instant crowds to draw the police to an instant riot.

I think that all of us in the IT, network and security fields are used to critical thinking. We have to be to keep up with the flood of technical information and distinguish marketing exaggerations from realistic information. We are used to writing and reading product comparisons, strategy evaluations and management recommendations as part of our work. Let's use our skills to foster critical thinking throughout the educational system. Let's work as volunteers on school boards, in the classroom and in social organizations to introduce critical thinking to children and adults who haven't learned how to distinguish reality from propaganda. Push for curriculum changes to accompany lessons on how to use the Internet with lessons on how to weigh the information found through e-mail and on the Web.

Let's make sure that we're not patsies for an information warfare attack rooted in disintermediated propaganda.

\* \* \*

For further reading

Agre, P. (1998). Phil Agre talks more about disintermediation. < http://www.xent.com/FoRK-archive/august98/0321.html >

Webopedia (2004). Disintermediation.

< http://www.webopedia.com/TERM/D/disintermediation.html > Bosworth, S. (2002). Information Warfare. Chapter 7 from \_Computer Security Handbook, 4th Edition\_, Bosworth, S. & M. E. Kabay, eds. Wiley (New York). ISBN 0-471-41258-9. xxiv + 1184. Index.

Campen, A. D., D. H. Dearth, & R. T. Goodden, eds. (1996). \_Cyberwar: Security, Strategy, and Conflict in the Information Age\_. AFCEA International Press (Fairfax, VA). ISBN 0-916-15926-4. vii + 296.

Gordon, S., R. Ford & J. Wells (1997). Hoaxes & hypes. Presented at the 7th International Virus Bulletin Conference. http://www.research.ibm.com/antivirus/SciPapers/Gordon/HH.html

Henry, R. & C. E. Peartree (1998), eds. \_The Information Revolution and International Security\_. Center for Strategic and International Studies (Washington, DC). ISBN 0-892-06299-1. xx + 194. Index.

Kabay, M. E. (1995). Information Warfare.

< http://www2.norwich.edu/mkabay/overviews/infowar\_1995.htm > or

< http://www2.norwich.edu/mkabay/overviews/infowar\_1995.pdf >

Kabay, M. E. (2003). Cyber-Safety for Everyone: from Kids to Elders, Second Edition. Accura Printing (Barre, VT). ISBN TBD. vi + 124. In press. Also available free from http://www2.norwich.edu/mkabay/cyberwatch/cybersafety.pdf

Kuehl, D. (2000). Statement to the Joint Economic Committee of the Senate of the United States. < http://www.cdt.org/security/dos/000223senate/kuehl.html >

Kuehl, D. (2004). Information Warfare: What it Is, Isn't and How It Shapes National Security. Slide show from January 23, 2004 presentation at New York Military Affairs Symposium. < http://libraryautomation.com/nymas/infowarfare2004.htm >

Lesser, I. O., B. Hoffman, U. Arquilla, D. Ronfeldt & M. Zanini (1999). \_Countering the New Terrorism\_. RAND Corporation Report

< http://www.rand.org/publications/MR/MR989/ > Also available as a printed document, ISBN 0-833-02667-4 through online purchase.

Schwartau, W. (1996). \_Information Warfare, Second Edition\_. Thunder's Mouth Press (New York). ISBN 1-560-25132-8. 768. Index.

Category 29.6 Flash crowds, social e-links

2004-05-13 friends social networking cellular mobile phone text message

http://www.nytimes.com/2004/05/13/technology/circuits/13dodg.html

SOCIAL NETWORKING THROUGH CELL-PHONE TEXT-MESSAGING

Users of cell-phone based text-messaging services for social connections such as Dodgeball.com find it convenient to meet people who are friends of their friends. Some 5,000 people signed up in New York City, Boston, Philadelphia, San Francisco and Los Angeles within about a month from its introduction.

[MK notes: This system, were it to be hacked, could be misused to trick people into becoming victims of Bad People — thieves, stalkers, rapists and so on. I hope we will be hearing more about security measures to prevent damage to the databases on which the affinity relations are based.]

Category	29.6	Flash crowds, social e-links
----------	------	------------------------------

#### 2004-07-06 Los Angeles cybercafes close computer crime cybersyndrome

NewsScan

L.A. TO CLEAN UP CYBERDENS OF INIQUITY

The Los Angeles City Council members have voted unanimously to regulate cyber cafés where teens and others hang out to use computers. The proposal was introduced after a string of shootings at cyber cafés, but council members say it is not their intention to drive the cafés out of business.

One 14-year-old patron says: "Most people can't afford computers that work this good. At least we're being social here instead of staying at home." (Los Angeles Times 6 Jul 2004)

Category 29.6 Flash crowds, social e-links

2004-07-29 Wiki wikipedia online encyclopedia information spread source disintermediation

NewsScan

THE WIKI WAY TO COMMUNICATE

A wiki (the Hawaiian word for 'quick') is a type of Web site that many people can revise, update and append with new information. Whereas blogs are essentially designed for personal expression, wikis are designed for collaboration. The concept was pioneered in the mid-1990s by programmer Ward Cunningham, who called it the WikiWikiWeb and intended it to serve as a platform for freewheeling collaboration in software and engineering projects. Ross Mayfield of the Silicon Valley startup called Socialtext says: "People have tried very hard to take fragmented knowledge within

corporations and put it somewhere that it can be used, but it's been an uphill effort. Our focus is literally to get everyone on the same page." And New York University communications professor Clay Shirky explains that "people are realizing that perhaps the most human value actually occurs in

smaller groups." (Wall Street Journal 29 Jul 2004)

Category 29.6 Flash crowds, social e-links

#### 2004-08-17 California cyber café violence gang gathering activity

NewsScan

VIOLENCE AT CALIFORNIA'S CYBERCAFES

Episodes of violence at several businesses in southern California have prompted a number of municipal crackdowns -- the latest of which is taking the form of a Los Angeles ordinance requiring that the city's 30 Internet cafes enforce the city's long-standing curfew for minors, pay for in-store

surveillance cameras, enforce limits on how many computers each business can operate, and obey prohibitions against dark window coverings. But Ernest Miller, a spokesman for iGames, which represents about 500 PC gaming parlors in the U.S. and abroad, insists that there's nothing particularly violent about cybercafes: "A haven for gang activity can be any location where people gather -- corner liquor stores, pool halls or cinemas." (AP/San Jose Mercury News 17 Aug 2004)

Category29.6Flash crowds, social e-links2004-10-27blogs weblogs fasion advertising discussion forms ideas data leakage confidentiality

NewsScan; http://www.nytimes.com/2004/10/27/business/media/27adco.html

MADISON AVENUE WAKES UP TO WEB LOGS

Advertising agencies and communications professionals are testing the effectiveness of using blogs to create forums for discussion about ideas within their industries, with topics ranging from video game marketing to the art of client service. However, the biggest agencies are still holding out, noting that the potential risks still outweigh the benefits. "Blogs are in fashion, and it is easy to hop on the bandwagon and say that every company should have one," says an executive with Deutsch, a unit of the Interpublic Group of Companies. "The questions any smart marketer should be asking are, 'Does this provide a platform to connect with their most relevant audiences and how will this address business objectives?' That's not to say we would never enter blogland, but there is a fine line between being timely, topical and keeping current while making sure that we are doing what's best for our business long term." The biggest risk, say many experts, is an uncontrolled message slipping out and damaging the company. But it's clear that as blogging evolves into a corporate tool, it's also losing those qualities that made it such a hit in the first place: attitude, irreverence and a penchant for kicking up a ruckus. (New York Times 27 Oct 2004)

 Category
 29.6
 Flash crowds, social e-links

 2004-11-15
 RFID radio freqency identifier nTAG infrared

 NewsScan;
 http://www.boston.com/business/technology/articles/2004/11/15/breaking\_the\_ice

 20/
 20/

HELLO, I'M A DOG LOVER, TOO!

Schmoozing at big corporate events can be painful for the socially challenged, but now there's the nTAG -- an electronic name tag that beams messages to fellow conventioneers like, "Hi, Jane, I like strawberry ice cream, too." The device uses infrared sensing and radio frequency identification to communicate with other tags and it lights up in the dark for those who do their networking at the bar. "People want a reason to interact," says nTAG inventor Rick Borovoy. "They need help. This gives them a powerful nudge in that direction." Meeting participants have given the nTAG high marks for being an icebreaker that helps them circulate beyond their usual pool of friends or colleagues, and meeting planners use the data collected to evaluate session popularity and exhibit attendance. (Boston Globe 15 Nov 2004)

## **31.1 Surveys, studies, audits of security**

Category 31.1 Surveys, studies, audits of security

#### 2004-01-12 computer crime risk Ukraine illegal access hackers library archive resource

NewsBits; http://www.crime-research.org/library/Golubev1203.html

A Ukrainian criminologist published a review of computer-crime classifications from the point of view of law enforcement specialists in the former Eastern Bloc. Of special interest is the Web site that collected his article: The Computer Crime Research Center at < http://www.crime-research.org/>, which files hundreds of articles per year starting in July 2002.

Category 31.1 Surveys, studies, audits of security

#### IP network attack easy report survey estimate infrastructure protection

DHS/IAIP Update

2004-01-20

January 15, CNET News — Report: IP networks easy prey for cyberattackers.

The increasing use of Internet Protocol (IP) technology in power stations, railroads, banks and other critical infrastructure could spell big trouble, and soon, according to analysts. Although an actual act of cyberterrorism or cyberwarfare has never been recorded, the potential exists and is being facilitated by an increasingly connected world, according to a report released on Wednesday, January 14, by market- research firm Gartner. Cyberwarfare could be a reality by 2005, the company said. Technologies such as VoIP and the trend towards voice and data convergence give benefits cost and flexibility to businesses, but they also expose vital telecommunications networks to traditional forms of Internet attack, such as worms and viruses, according to the report. Gartner claims that, unlike traditional circuit- switched networks, VoIP networks have an inherent weakness when it comes to latency- - any delay to the packets carrying the voice traffic disrupts communication. A massive denial- of- service attack could "degrade call performance by slowing voice packet arrival at a given destination" and effectively cut off voice communication, the report says. Other weaknesses flagged include the Supervisory Control and Data Acquisition interfaces used to connect a significant portion of critical infrastructure elements such as dams, railroads, electrical grids and power stations.

## Category31.1Surveys, studies, audits of security2004-01-22electronig e-voting Internet-voting Department of Defense DoD SERVE Secure<br/>Electronic Registration and Voting Experiment flaw

RISKS

23 14

PANEL REPORTS DOD SERVE SYSTEM FATALLY FLAWED - BUREAUCRATS IN DENIAL

Scott Miller cites a \_Computerworld\_ article on the flaws of SERVE, a Pentagon secure e-voting project. Speaking about SERVE, Dr. Aviel D. Rubin, the technical director of John Hopkins' Information Security Institute said: "I think that a dedicated and experienced hacker could subvert the election rather easily..." SERVE spokesperson Glen Flood maintained: "The only 100% way we can avoid some of the security issues [raised by the four panel members] is to not do this. And that is not something we will do..." In a follow-up article, contributor Lillian Coney reported that political party organizations for emigrant Americans opposed SERVE by sending a joint letter to many congressional committees. She writes that about 100,000 from 50 counties were set to be case using SERVE.

Category 31.1	Surveys, studies, audits of security		
2004-02-12	terrorism detection system problems bugs fasle pos	itives reliability audi	t analysis
RISKS; http://www.latimes.com/technology/la-na-		23	19
profiling12feb12,1,3293045.story?coll=la-headlines-technology			

#### GAO REPORT WARNS OF AIRLINE SECURITY SHORTCOMINGS

In its report (released on 13 Feb 2004), a General Accounting Office study notes that CAPPS II (intended to pick out potential terrorists from among millions of air passengers) has run into "significant challenges" posing "major risks" to its deployment and public acceptance. Problems include overall system reliability and false positives, and resolving the rights of those falsely identified. Passenger-provided information would be outsourced to government contractors for analysis, the government would check supposedly validated identities against a watch list, and the result would be a green, yellow, or red risk rating for each would-be passenger. Allegedly only about 4% would be rated yellow, and "an average of only one or two people a day" would be rated red. [Remember that even a 1% false positive rate would mistakenly identify tens of thousands of travelers.]

"But the GAO report found that the agency has not adequately addressed seven of eight concerns raised by Congress. These include preventing abuses, protecting privacy, creating an appeals process, assuring the accuracy of passenger data, testing the system, preventing unauthorized access by hackers and setting out clear policies for the system." GAO investigators concluded that, though the agency was making advances in all these areas, progress was incomplete.

[This abstract was prepared by Peter G. Neumann.]

Category31.1Surveys, studies, audits of security2004-02-25Hotels broadband Internet access vulnerability STSN Windows file sharing

DHS IAIP Daily; http://edition.cnn.com/2004/TRAVEL/02/25/biz.trav.security/

February 25, CNN — Hotel networks face hacker threat.

Many hotels have added high- speed wireless connections for executives to surf the Internet or access corporate data on the road. However, with security software available on the Internet from sites like www.insecure.org, hackers can explore unsecured hotel networks and tap into a guest's laptop computer. "Most hotels claim to offer secure broadband services, but most do not know enough about security issues to ask their providers the right questions," David Garrison of STSN, a broadband security firm told CNN. The biggest problem is that many laptops using Microsoft Windows have a default setting that enables you to share files or communicate with other computers. Unfortunately, unless this is turned off hackers can easily get in when you log on to a wireless network. The key thing is to ask your hotel about security before booking a room and to only use those that use reputable security systems. Personal firewalls can be used as a deterrent. These are software- based and simple versions can be downloaded for free online. There are a few other steps executives can take to boost their security while using VPNs on the road, according to Garrison. "Install an anti- virus program, turn off file- sharing capabilities and make sure you have the latest security updates for your operating system," he explained.

Category 31.1 Surveys, studies, audits of security

#### 2004-02-25 software movie digital piracy Australia costs

NewsScan

PIRACY COSTS INDUSTRY \$AU160 MILLION

Video and computer game piracy in Australia costs the industry there at least \$AU160 million a year. A new study, "Australian Crime: Facts and Figures 2003" found that the illegal market accounted for one in 12 movies sold in Australia. Software piracy accounts for around one-third of the market, costing the industry \$AU138.5 million in 2002. (The Australian 25 February 2004)

Category 31.1 Surveys, studies, audits of security

#### 2004-03-03 **4-1-9 Nigerian advance fee fraud Britain statistics**

http://www.theregister.co.uk/2003/03/03/150\_brits\_x\_419\_fraud/

In 2002, more than 150 Britons admitted being fleeced by the Nigerian 4-1-9 advance-fee fraud. Total report lost: £8.4M. Average loss reported: £56K.

Category 31.1 Surveys, studies, audits of security

#### 2004-03-17 anti-spam law failure CAN-SPAM act

NewsScan

ANTI-SPAM LAW GOES SPLAT

A new survey from the Pew Internet & American Life organization reports the following findings: 63% of e-mail users who responded to the survey think that spam has made them less trusting of e-mail as a communications tool, and 77% think that spam makes being online "unpleasant and annoying." [The respondents obviously don't get NewsScan Daily.] A spokesperson for Senator Ron Wyden (D, OR), who co-sponsored the federal "Can-Spam Act," says: "It's premature to judge the effectiveness of the Can-Spam Act 77 days after it becomes effective. It's not time to write Can-Spam's obituary." Doug Peckover of Privacy Inc. suspects that the people spam is driving away are probably the "fringe" Internet users, who "don't depend on it for business, and for them, their pain threshold is a lot lower than for you and me. These are the folks who are saying, 'You know, it's not worth it anymore.'" (Washington Post 17 Mar 2004)

Category 31.1 Surveys, studies, audits of security

#### 2004-03-29 music piracy study survey RIAA industry claims wrong

NewsScan

STUDY CONTRADICTS MUSIC INDUSTRY'S PIRACY CLAIMS

Two university researchers have released a study that indicates online music piracy has no negative effect on legitimate music sales, and in fact boosts sales in some cases. "Consumption of music increases dramatically with the introduction of file sharing, but not everybody who likes to listen to music was a music customer before, so it's very important to separate the two," says Felix Oberholzer-Gee, an associate professor at Harvard Business School, who co-authored the study. Oberholzer-Gee and his colleague, University of North Carolina professor Koleman Strumpf, say their "most pessimistic" statistical model indicates that only 2 million CD sales were lost due to illegal file-sharing in 2002, whereas CD sales declined by 139 million units between 2000 and 2002. "From a statistical point of view, what this means is that there is no effect between downloading and sales," says Oberholzer-Gee. The study's results contradict the recording industry's assertions that their financial decline is attributable in large part to music piracy, citing several studies that have supported that claim. However, some other research groups said the Harvard-UNC study conclusions appeared to mirror their own research findings. "While some people seemed to buy less after file sharing, more people seemed to buy more," says Jupiter Research analyst Aram Sinnreich, who conducted similar studies in 1999 and 2002. (Washington Post 29 Mar 2004)

Category 31.1 Surveys, studies, audits of security

#### 2004-04-13 IT professionals grade vendor software standards poorly

DHS IAIP Daily; http://fcw.com/fcw/articles/2004/0412/web- survey- 04- 13- 04.as p

April 13, Federal Computer Week — IT pros see vendor mediocrity.

Six hundred federal information technology professionals surveyed in January graded the performance of manufacturers, integrators and resellers they do business with at about a C+ average, according to the survey from Market Connections Inc. The report, released this week, states that on 15 performance factors, no one factor got an average score higher than a B-. Forty- six percent of the respondents reported using a credit card to purchase IT products online, with an average purchase under \$2,500 for more than half of those surveyed. The survey found that the respondents believe IT security and information sharing among agencies will be the most important initiatives in the immediate future to help agencies fulfill homeland security missions.

Category 31.1 Surveys, studies, audits of security

#### 2004-04-13 browser attacks increase CompTIA survey

DHS IAIP Daily; http://www.esecurityplanet.com/trends/article.php/3339731

April 13, eSecurity Planet — Browser- based attacks surging.

The Computing Technology Industry Association (CompTIA), a global trade association based in Oakbrook Terrace, IL, reports that a new survey of 900 organizations shows that browser- based attacks are surging, and may pose the 'next significant security threat' to enterprise networks. The study reports that 36.8 percent of the companies surveyed suffered a browser- based attacks in the last six months. That number is up 25 percent from when the same study was conducted last year. These attacks, which are related to the recent spate of phishing scams, use a browser and user system permissions to allow an attacker to gain access to the computer to steal or destroy critical information. The attacks generally occur when a user visits a Website that, on the surface, appears harmless, but contains malicious code that convinces the browser to execute commands designed to sabotage the machine or lift proprietary data or personal financial information. The Computing Technology Industry Association also reports that while incidents of browser- based attacks are on the rise, computer viruses and worm attacks still far outweigh them. The survey shows that 68.6 percent say viruses and worms are the most security threat they have to deal with.

Category 31.1 Surveys, studies, audits of security

#### 2004-04-16 Cisco security warning IPSec VPN PKI threat

DHS IAIP Daily;

http://news.com.com/2100-7355\_3-5193521.html?tag=nefd.top

April 16, CNET News.com — Cisco issues another security warning.

Cisco Systems warned customers on Thursday, April 15, of what security experts are calling a "minor security issue" in its IPSec- based VPN 3000 Concentrator. The problem, which is present in both Linux and Microsoft versions of the IPSec client, occurs when customers configure the VPN (virtual private network) concentrator to accept group passwords rather than digital certificates for authentication. Typically, a group password is encrypted when used for authentication. But on VPN 3000 Concentrator clients, the password can be extracted from memory, making it available to anyone using a device with the Cisco software client. People who have gained knowledge of a group password may use it to hijack connections or gain knowledge of sensitive information when these are used as pre- shared keys during authentication. Cisco recommends that customers deploy PKI (Public Key Infrastructure) instead of a Group Password based authentication scheme. Additional information is available on the Cisco Website:

http://www.cisco.com/warp/public/707/cisco- sn- 20040415- grppa ss.shtml

Category 31.1 Surveys, studies, audits of security

#### 2004-04-26 music piracy copyright infringement lawsuits P2P peer-to-peer

NewsScan

PEW REPORTS DECLINE IN MUSIC DOWNLOADINGS

A new report from the PEW Internet and American Life Project indicates that the lawsuits brought by Recording Industry Association of America (RIAA) against are having a definite impact on Internet music downloaders. A phone survey in February shows that 14% of online Americans (17 million people) say that at some time in their online lives they downloaded music files but no longer do any downloading. The Pew reports also says that new data from comScore Media Metrix show continuing declines or stagnation in the number of people with popular peer-to-peer file sharing applications actively running on their computers. (Pew Internet Project 26 Apr 2004) Category 31.1 Surveys, studies, audits of security

#### 2004-04-28 survey study UK business vulnerable security IT skills lacking

DHS IAIP Daily; http://www.vnunet.com/News/1154752

April 28, vnunet.com (UK) — UK businesses still vulnerable to security breaches.

A lack of IT security skills is leaving UK businesses vulnerable to security breaches, according to research. The Department of Trade and Industry Information Security Breaches Survey 2004 suggests that 89 per cent of companies say staff have no formal IT security qualifications. The study, by PricewaterhouseCoopers (PwC), says there is an average of one security incident per month in UK firms, but one a week in large companies. Three- quarters of UK companies, and 94 per cent of large organisations, suffered a security incident in the last year. Human error is the cause of most problems, but only a third of businesses have a security policy in place. Security spending has increased since the last survey in 2002, but only slightly from two per cent to three per cent of the annual IT budget. The report says this is well below the five to 10 per cent benchmark level. The study is available online:

http://www.security- survey.gov.uk/

Category 31.1 Surveys, studies, audits of security

#### 2004-05-18 **financial sector external threats**

DHS IAIP Daily; http://continuitycentral.com/news01223.htm

May 18, Continuity Central — Financial institutions struggling to fend- off escalating security threats.

The majority of global financial institutions have had an external attack on their information technology systems within the last year and many of these breaches resulted in financial loss, according to Deloitte's 2004 Global Security Survey. However, even with security attacks on the rise, the largest number of respondents (some 25 percent) reported flat security budget growth. According to the survey, the vast majority (83 percent) of respondents acknowledged that their systems had been compromised in the past year, compared to only 39 percent in 2002. Of this group, 40 percent stated that the breaches had resulted in financial loss to their organization. The survey also finds that companies are sliding backwards when it comes to the use of security technologies. While more than 70 percent of respondents perceived viruses and worms as the greatest threat to their systems in the next 12 months, only 87 percent of respondents had fully deployed anti- virus measures. This result is down from 96 percent in 2003. Report: http://www.deloitte.com/dtt/research/0,2310,sid%253D1013%252 6cid%253D48978,00.html

Category 31.1 Surveys, studies, audits of security

2004-05-18 kids downloading music internet access copyiright computer viruses songs

NewsScan

SURPRISE — KIDS ARE STILL DOWNLOADING MUSIC

Fifty-six percent of American children ages eight to 18 with Internet access are continuing to download music, even though 88% of the respondents polled indicated they were familiar with music copyright restrictions, according to a new survey by Harris Interactive. The survey noted that more kids worry about downloading computer viruses with their songs than about getting in trouble with the law. The Harris poll was commissioned by the Business Software Alliance, which said the responses indicate a need for the software and entertainment industries to step up their efforts to dissuade kids from file-sharing. "It's a very good sign that a lot of kids and youth understand that creative works are protected by copyright law. [But if] they're still doing the wrong thing, that's not good," said a BSA spokeswoman. A spokesman for the Recording Industry Association of America, which has led an aggressive campaign against illegal music downloading, said the latest numbers show that "education is important, but without an enforcement component, it can only do so much to influence behavior." Meanwhile, the executive of a P2P networking company suggested it would be more productive to find ways for the two sides to cooperate rather than clamp down on music distribution. (Washington Post 18 May 2004)

Category 31.1	Surveys, studies, audits of security
2004-05-24	online crime cybercrime scams phishing identity theft

DHS IAIP Daily;

http://www.washingtonpost.com/wp- dyn/articles/A53042- 2004May 24.html

May 24, The Washington Post — Study: Online crime costs rising.

Online criminals are attacking corporate and government networks more frequently, costing businesses an estimated \$666 million in 2003, according to a survey of computer security executives released Monday, May 24. The survey was conducted by CSO [Chief Security Officer] magazine in cooperation with the U.S. Secret Service and the CERT cybersecurity center. More than 40 percent of 500 executives polled said hackers have become the greatest cybersecurity threat to business and government networks. Computer systems falling prey to ever more sophisticated attacks are increasingly essential to the daily operations of businesses and government agencies, said Harris Miller, president of the Information Technology Association of America (ITAA). ITAA has long warned that many companies have not devoted enough time and money to cybersecurity. A taskforce reported to the Department of Homeland Security in April that most corporations fail to take cybersecurity seriously at the top levels of management. The report did not recommend that the government make cybersecurity a requirement for the private sector, but said that auditing firms should include cybersecurity readiness as part of the criterion for determining whether companies have adequate internal and financial safety controls.

Category 31.1 Surveys, studies, audits of security

2004-05-25 authors source of viruses Russia organized crime denial of service DoS extortion

DHS IAIP Daily;

http://www.infoworld.com/article/04/05/25/HNrussianviruses\_1.html

May 25, IDG News Service — Viruses nip Russia after the Cold War.

For all its disadvantages, the former Soviet Union had one hugely overlooked advantage: it kept hackers, crackers and virus writers confined inside the country by restricting their access to the Internet. A decade later, Internet penetration is booming in the region, particularly in Russia, and viruses are epidemic. Russians are linked to some of the nastiest viruses the IT world has ever experienced: Bagel, MyDoom and NetSky, to name just a few. Security experts warn that the situation is likely to worsen as hacking, cracking and virus writing shift from being a mischievous hobby of young kids to a lucrative occupation of skilled professionals working hand- in- hand with hardened criminals. The motive is obvious: money- - in some cases, big money, which fuels other traditional Mafia activities, such as drug smuggling and prostitution. Today, hundreds or even possibly thousands of skilled Russians desperate for cash are scouring the Internet looking for security vulnerabilities in the computer networks of companies, particularly in the U.S. and Europe. They are creating worms and Trojans for stealing credit card and other financial information, or turning inflected computers into zombie hosts to establish illegal spam farms, or extorting money by threatening companies with a distributed denial- of- service attack if they don't pay.

Category 31.1 Surveys, studies, audits of security

### 2004-09-03 CIO Council federal managers information security privacy guidelines

DHS IAIP Daily;

http://www.fcw.com/fcw/articles/2004/0830/web- fea- 09- 03- 04.asp

September 03, Federal Computer Week — CIO Council releases info- sharing guide.

Federal managers received new policy guidelines this week to help them minimize risks when sharing sensitive information online. The guidelines, issued by the federal Chief Information Officers Council, are supposed to help federal decision- makers balance the often- conflicting demands to guarantee information security and privacy and against demands to carry out their agencies' missions. For federal managers who are developing new information systems, the guidelines urge thinking about data privacy and data security as early as possible and at the highest levels possible. In an era of extensive information sharing, "information assurance specialists by themselves can no longer be charged to protect enterprise resources," the guidelines state. If agency managers follow the guidelines, they will find security and privacy controls affecting all aspects of information systems development and operations, including how they measure their systems performance, engineer workflow, design directory information, achieve interoperability and exchange data.

Category 31.1 Surveys, studies, audits of security

2004-09-06 Internal Revenue Service IRS federal US government govt. security audit

DHS IAIP Daily; http://www.computerworld.com/securitytopics/security/story/0,10801,95705,00.html

September 06, Computerworld — Federal audit raises doubts about IRS security system.

Software performance and functionality problems continue to plague the Security Audit and Analysis System (SAAS) designed to detect hacking and other unauthorized activities on computers at the Internal Revenue Service, according to auditors within the U.S. Department of the Treasury. The problems are limiting the ability of business managers and IT security workers at the IRS to identify improper uses of new applications that provide online tax services and information about refunds, the auditors said in a report issued last month by the Office of the Treasury Inspector General for Tax Administration. "Not having an effective audit- trail review process is a significant security weakness that should weigh heavily on whether to accredit future modernization applications," the report said. Daniel Galik, chief of mission assurance for the IRS, said that the system met all defined requirements and passed all tests before it was accepted. Galik wrote that the IRS is taking steps to correct the system problems and expects all the major components of SAAS to be fully functional by the end of October.

### Category31.1Surveys, studies, audits of security2004-09-20online atacks rise study survey Internet Security Threat Report Symantec botnets

NewsScan

INTERNET ATTACKS JUMP SIGNIFICANTLY THIS YEAR

spammers vulnerabilities

The semiannual Internet Security Threat Report, which is based on monitoring by computer security firm Symantec, indicates that in the first six months of 2004 there were at least 1,237 newly discovered software vulnerabilities and almost 5,000 new Windows viruses and worms capable of

compromising computer security. The numbers represent a dramatic increase over the same period in 2003. Even more troubling was the sharp rise in the number of "bot," or robot, networks, which comprise a large number of infected PCs that can then be used to distribute viruses, worms, spyware

and spam to other computers. The survey notes that in the first half of 2004, the number of monitored botnets rose from fewer than 2,000 to more than 30,000. The botnets, which range in size from 2,000 to 400,000 "zombie" machines, are often "rented out" to commercial spammers who use

them to distribute junk e-mail while concealing their identities. E-commerce was the industry most frequently targeted for attacks, accounting for 16% of the total, and report authors note that phishing

scams are responsible for pushing up the numbers in that category. "We're seeing a professional hand in development that was pretty startling in terms of malicious code," says Alfred Huger, senior director of engineering for security response at Symantec. The report's findings mirror those of

recent government-supported research. (New York Times 20 Sep 2004)

Category 31.1 Surveys, studies, audits of security

### consumer cyberattacks attitude light National Cyber Security Alliance

DHS IAIP Daily;

2004-09-30

http://news.com.com/Study%3A%2BConsumers%2Btake%2Bcyberattac ks%2Blightly/2100-7349\_3-5390749.html

September 30, CNET News.com — Study: Consumers take cyberattacks lightly.

Consumers have a casual approach toward cybersecurity and fail to grasp the pervasiveness of online threats, according to a study release Thursday, September 30, by the non- profit National Cyber Security Alliance (NCSA). The results of a major study on cybersecurity are due in October. The NCSA has dubbed October as National Cyber Security month and will spend the month attempting to educate users.

## Category 31.1 Surveys, studies, audits of security 2004-10-24 cybersecurity survey America Online AOL spyware virus awareness education training firewall vulnerability

NewsScan;

 $http://news.com.com/Plague+carriers+Most+users+unaware+of+PC+infections/2100-1029\_3-5423306.html$ 

CYBERSECURITY LARGELY IGNORED BY INDIVIDUAL USERS

A new study by America Online and the National Cyber Security Alliance indicates that about 80% of home PCs are infected with spyware, but most users aren't even aware of it. And while 85% of users had installed antivirus software, two-thirds of those had not updated it in the past week. In addition, about 20% had an active virus on their machines and two-thirds did not have a firewall installed. AOL chief trust officer Tatiana Gau says the results highlight just how vulnerable the average online user is to malicious hackers. "No consumer would walk down the street waving a stack of cash or leave their wallet sitting in a public place, but far too many are doing the exact same thing online. Without basic protections like antivirus, spyware and firewall software, consumers are leaving their personal and financial information at risk." (CNet News. com 24 Oct 2004)

Category 31.1 Surveys, studies, audits of security

### 2004-10-25 Internet security weak survey report AOL NCSA DHS FTC

DHS IAIP Daily;

http://www.washingtonpost.com/wp- dyn/articles/A60199- 2004Oct 25.html

October 25, Associated Press — Security for Internet users deemed weak.

Internet users at home are not nearly as safe online as they believe, according to a nationwide inspection by researchers. They found most consumers have no firewall protection, outdated antivirus software and dozens of spyware programs secretly running on their computers. The study released Monday, October 25, by America Online (AOL) and the National Cyber Security Alliance (NCSA) found that 77 percent of 326 adults in 12 states assured researchers in a telephone poll they were safe from online threats. When experts visited those same homes to examine computers, they found two- thirds of adults using antivirus software that was not updated in at least seven days. Two- thirds of the computer users also were not using any type of protective firewall program, and spyware was found on the computers of 80 percent of those in the study. The survey participants all were AOL subscribers selected in 22 cities and towns. NCSA, a nonprofit group, is backed by the Homeland Security Department and the Federal Trade Commission, plus leading technology companies. Study: http://www.staysafeonline.info/home- news.html

Category 31.1 Surveys, studies, audits of security

### 2004-10-28 Department Homeland Security DHS information security deficiency report negative

DHS IAIP Daily;

http://www.fcw.com/fcw/articles/2004/1025/web- dhsig- 10- 28- 04 .asp

October 28, Federal Computer Week — Report: DHS has 'significant deficiency' in info security.

The Homeland Security Department's (DHS) inspector general (IG) has completed an information security audit of the agency, which shows DHS officials are still struggling with internal cybersecurity issues. The report, released Wednesday, October 27, highlights areas in which DHS officials have improved the department's information security practices and policies. But the overall tone of the report is negative. The report cited the chief information officer's lack of authority to manage DHS' departmentwide information technology programs and spending as a significant factor in the department's struggle to secure its information systems. Steven Cooper, DHS' CIO, stated that while he generally concurred with the IG's findings, DHS officials have begun a comprehensive inventory of general support systems and major applications and will review data captured in the agency's automated systems. Report: http://www.dhs.gov/dhspublic/interweb/assetlibrary/OIG\_04- 41 .pdf

### Category31.1Surveys, studies, audits of security2004-11-01laptop portable security concern lax Europe survey lack of policy

DHS IAIP Daily;

http://www.techworld.com/security/news/index.cfm?NewsID=2517

November 01, Techworld — Lax laptop policies create security concerns.

A new Europe- wide survey has revealed that laptops returning to company networks after their travels are now one of the biggest security hazards faced by many companies. Despite this, 70 percent of companies questioned offered no written guidance to employees on the use of their machines, and only a quarter imposed technological restrictions. The survey of employees in 500 companies across Europe on behalf of Websense, uncovered the tendency of many employees to treat laptops as unofficial personal possessions. As an absolute minimum, companies should start asking employees to sign up to reasonable use guidelines, while IT staff should treat any laptop connecting to the company network after returning from its travels as a major security risk.

Category 31.1 Surveys, studies, audits of security

### 2004-11-05 e-governance e-voting UK Ireland Uganda

NewsScan; http://www.washingtonpost.com/wp-dyn/articles/A27612-2004Nov5.html?nav=headlines

E-GOVERNANCE FACES CHALLENGES ABROAD

Many overseas e-governance projects are failing, due to poor planning, political interference and bureaucratic bungling, according to World Bank information technology specialist Robert Schware. E-governance refers to efforts by governments to use Internet and computer technology to provide services to citizens and businesses. Schware notes that about 35% of all such projects in developing countries are a washout, with an additional 50% failing in some respect, leaving only about a 15% success rate. Schware cites \$63 million spent by Ireland's government to test electronic voting technology before the project was abandoned due to doubts about its accuracy and privacy concerns. Uganda spent \$22 million on an e-voting system, which performed poorly at the polls in 2001. And the U.K. pursued a \$23.5 online university project that attracted only 900 students. One problem, says Schware, is that politicians sometimes want to speed up the timeline of the e-voting projects in order to win votes -- a process that usually ends up hurting the project. (AP/Washington Post)

Category 31.1 Surveys, studies, audits of security

2004-11-09 computer security information assurance IA jobs work survey study

WSJ;

INFOSEC Jobs on the Rise

IDC released a study in November 2004 showing that information assurance specialists continued to see growth in demand and salaries. Combinations of technological knowledge and business acumen were particularly highly in demand.

Category 31.1 Surveys, studies, audits of security

### 2004-11-16 hackers getting better attack boom Internet security VeriSign

DHS IAIP Daily; http://www.techweb.com/wire/security/53200186

November 16, TechWeb News — Better hackers behind attack boom according to Internet security firm.

Security events in the third quarter jumped 150 percent over the same period last year, fueled by more sophisticated hackers writing better code who are more interested in dollars than creating computer disasters, said Internet security firm VeriSign in a new report issued Tuesday, November 16. Hackers are not only getting bolder, but they're getting better at their "jobs," said Mark Griffiths, VeriSign's vice president of security services. "Viruses written to be malicious didn't need to be written very well, but now that their primary aim is money, they're writing better code," Griffiths said. That has had a direct impact on not only the sophistication of attacks, but also their number. Sample exploits, notes VeriSign in the report, once were of such poor quality that only a skilled programmer could edit the code to produce a working attack. In the past quarter, however, exploit code has been surprisingly simple to make work, which gives less technically- astute hackers a much better chance of wrecking havoc themselves as they massage the exploit code into a working worm or virus. Report: http://www.verisign.com/static/017574.pdf

Category 31.1	Surveys, studies, audits of security
2004-11-30	information security training government employees importance

DHS IAIP Daily;

http://www.fcw.com/geb/articles/2004/1129/web- secure- 11- 30- 0 4.asp

November 30, Federal Computer Week — Stressing security training.

Teaching basic computer security has become an essential part of training government employees, and agency officials who neglect security education will regret it, said David Jordan, chief information security officer for Arlington County, VA. Employees who are aware of the pitfalls of using computers connected to the Internet are "the most powerful weapons against cyberthreats that you can have," Jordan said. He spends 15 to 20 minutes with all new county government employees talking to them about cybersecurity. And it's why he sends computer and network security information to employees on a biweekly basis via the county's electronic newsletter. Editors can help take a security officer's message and craft it to suit to the audience, Jordan said.

Category	31.1	Surveys,	studies.	audits o	f securit	V

2004-12-17 Department of Homeland Security DHS cyber security lagging report NIST guidelines NSA recommendations

DHS IAIP Daily; http://www.securityfocus.com/news/10148

December 17, SecurityFocus — Report: DHS cyber security lagging.

The U.S. Department of Homeland Security (DHS) is having some homeland cyber security issues on its systems providing remote access to telecommuters, according to a newly- released report by the DHS Inspector General's office. Earlier this year security auditors spent five months probing hosts, attacking passwords and war dialing the Department. They found that some of the hosts designed to allow home workers and other trusted users access to DHS networks by modem or over the Internet lacked the authentication measures called for by official NIST guidelines and recommendations by the National Security Agency. The Inspector General's report recommends that DHS update the DHS Sensitive Systems Handbook to include implementation procedures and configuration settings for remote access to DHS systems, ensure that procedures for granting, monitoring, and removing user access are fully implemented, and ensure that all necessary system and application patches are applied in a timely manner. While Department CIO Steve Cooper concurred with the recommendations, he said some of the auditors' concerns were overstated: The systems suffering known vulnerabilities were waiting for patches to come out of testing, and any genuine effort at password hacking would be hobbled by the Department's policy of limiting failed login attempts. Report: http://www.dhs.gov/dhspublic/interweb/assetlibrary/rOIG\_05- 0 3\_Nov04.pdf

# 31.2 Estimates, guesses, predictions, forecasts concerning security

Category 31.2 Estimates, guesses, predictions, forecasts concerning security

### 2004-01-06 open source database technology growth

NIPC/DHS; http://news.com.com/2100-7344-5134836.html

January 05, CNET News.com — Open-source databases gaining favor.

Big companies are warming up to open-source database software, according to a new study. "Concerns over stability, expense and how well a database plays with others are leading a quickly growing number of...companies to seriously consider and implement an open source database solution," says Evans Data analyst Joe McKendrick. "We expect this trend to continue as the open source offerings are continually improved upon." Database companies, also touting speed and the ability to handle very demanding processing tasks, have boosted efforts to make databases more reliable and cheaper to operate.

Category 31.2 Estimates, guesses, predictions, forecasts concerning security

### 2004-01-08 Anti-Spam Anti-Spyware Earthlink ISP security email blocking

NewsBits; http://www.internetnews.com/xSP/article.php/3296851

From Anti-Spam to Anti-Spyware: ISPs Beef Up their Defenses

Roy Mark reviewed efforts by Internet service providers (ISPs) to increase their customers' security and antispam capabilities. ISPs have been integrating measures to fight spyware, spam, viruses, pornography and hackers.

Category 31.2 Estimates, guesses, predictions, forecasts concerning security

### 2004-01-20 virus worm damage cost expense Trend Micro

NIPC/DHS; http://www.reuters.com/newsArticle.jhtml;jsessionid=K4R53JRC ZZC24CRBAEKSFFA?type=technologyNews&storyID=4138782

January 16, Reuters — Trend Micro says 2003 viruses caused \$55 billion damage.

Trend Micro Inc. said on Friday, January 16, that computer virus attacks cost global businesses an estimated \$55 billion in damages in 2003, a sum that would rise this year. Companies lost roughly \$20 billion to \$30 billion in 2002 from the virus attacks, up from about \$13 billion in 2001, according to various industry estimates. "The economic and financial impact of virus attacks will continue to climb in 2004," Lionel Phang, Trend Micro's Managing Director. Spam threats and network viruses will likely become more prevalent in 2004, he said. Blended threats also will remain the standard way to attack networks, where one virus file will create four to five different activities within the system." Viruses can also gain entry into computer networks via instant messaging channels, Phang added. "Spammers are going to put viruses and worms in email attachments, so (junk email) will become more than just a nuisance," said Natasha David, an analyst with International Data Corp. Analysts said the number of attacks between January and June 2003 exceeded 70,000, which is about twice the rate for 2002. "About 20 to 40 new and variant virus threats were reported to Trend Micro on a daily basis worldwide in 2003," Phang said.

Category 31.2 Estimates, guesses, predictions, forecasts concerning security

2004-01-20 virus worm damage cost expense Trend Micro

DHS/IAIP Update / Reuters

TREND MICRO SAYS 2003 VIRUSES CAUSED \$55 BILLION DAMAGE.

Trend Micro Inc. said on Friday, January 16, that computer virus attacks cost global businesses an estimated \$55 billion in damages in 2003, a sum that would rise this year. Companies lost roughly \$20 billion to \$30 billion in 2002 from the virus attacks, up from about \$13 billion in 2001, according to various industry estimates. "The economic and financial impact of virus attacks will continue to climb in 2004," Lionel Phang, Trend Micro's Managing Director. Spam threats and network viruses will likely become more prevalent in 2004, he said. Blended threats also will remain the standard way to attack networks, where one virus file will create four to five different activities within the system." Viruses can also gain entry into computer networks via instant messaging channels, Phang added. "Spammers are going to put viruses and worms in email attachments, so (junk email) will become more than just a nuisance," said Natasha David, an analyst with International Data Corp. Analysts said the number of attacks between January and June 2003 exceeded 70,000, which is about twice the rate for 2002. "About 20 to 40 new and variant virus threats were reported to Trend Micro on a daily basis worldwide in 2003," Phang said.

### IYIR 2004

## Category31.2Estimates, guesses, predictions, forecasts concerning security2004-01-20IP network attack easy report survey estimate infrastructure protection

NIPC/DHS; http://news.com.com/2100-7349-5141386.html?tag=cd\_top

January 15, CNET News - Report: IP networks easy prey for cyberattackers.

The increasing use of Internet Protocol (IP) technology in power stations, railroads, banks and other critical infrastructure could spell big trouble, and soon, according to analysts. Although an actual act of cyberterrorism or cyberwarfare has never been recorded, the potential exists and is being facilitated by an increasingly connected world, according to a report released on Wednesday, January 14, by market-research firm Gartner. Cyberwarfare could be a reality by 2005, the company said. Technologies such as VoIP and the trend towards voice and data convergence give benefits cost and flexibility to businesses, but they also expose vital telecommunications networks to traditional forms of Internet attack, such as worms and viruses, according to the report. Gartner claims that, unlike traditional circuit-switched networks, VoIP networks have an inherent weakness when it comes to latency—any delay to the packets carrying the voice traffic disrupts communication. A massive denial-of-service attack could "degrade call performance by slowing voice packet arrival at a given destination" and effectively cut off voice communication, the report says. Other weaknesses flagged include the Supervisory Control and Data Acquisition interfaces used to connect a significant portion of critical infrastructure elements such as dams, railroads, electrical grids and power stations.

Category 31.2	Estimates, guesses, predictions, forecasts concerning security
2004-02-01	outsourcing India globalization Wired

NewsScan

INDIA: THE NEW FACE OF THE SILICON AGE

An interesting long article in the new Wired magazine gives a good picture of India as it becomes the "new face of the Silicon Age." Journalist Dan Fink writes of Indian engineers doing outsourced programming work: "What begins to seep through their well-tiled arguments about quality, efficiency, and optimization is a view that Americans, who have long celebrated the sweetness of dynamic capitalism, must get used to the concept that it works for non-Americans, too. Programming jobs have delivered a nice upper-middle-class lifestyle to the people in this room. They own apartments. They drive new cars. They surf the Internet and watch American television and sip cappuccinos. Isn't the emergence of a vibrant middle class in an otherwise poor country a spectacular achievement, the very confirmation of the wonders of globalization — not to mention a new market for American goods and services? And if this transition pinches a little, aren't Americans being a tad hypocritical by whining about it? After all, where is it written that IT jobs somehow belong to Americans — and that any non-American who does such work is stealing the job from its rightful owner?" (Wired Feb 2000)

Category 31.2	Estimates, guesses, predictions, forecasts concerning security
2004-02-02	spam e-commerce adverse affect customers shoppers scared away Transatlantic Customer Dialogue

NewsScan

SHOPPERS SPOOKED BY SPAM

Spam is putting a damper on e-commerce, according to a survey published by the Transatlantic Consumer Dialogue, which indicates that 52% of respondents are shopping less on the Internet or not at all because of concerns that information disclosed in such transactions will generate more junk e-mail. "It is very clear that the majority of citizens are very troubled by unsolicited commercial e-mails. It is also very clear that bona fide businesses are losing money because the disreputable image of spam is making consumers uneasy about engaging in e-commerce." The results were released at an anti-spam summit held by the Organization for Economic Co-operation and Development (OECD), which is calling for international cooperation in tackling the scourge of spam and restoring consumer confidence in electronic commerce. "Most governments do view the Internet as a key to global economy. Spam certainly has the capacity to interfere with that," says Peter Ferguson, chairman of the OECD working party on information security and privacy. (Reuters/Washington Post 2 Feb 2004)

### IYIR 2004

Category 31.2	Estimates, guesses, predictions, forecasts concerning security
2004-04-23	grammar poor technology sociolinguistics SMS instant messaging IM

### NewsScan

### TECHNOLOGY MARCHES AHEAD, GRAMMAR GETS WORSE

Text messages, e-mail and the push for faster and more efficient communications are taking their toll on grammar, language experts believe. Queensland University of Technology sociolinguistics lecturer Jo Carr notes that people using e-mail and SMS text messaging are unconcerned about grammar and punctuation: "Grammar rules used to be an indication of social class and literacy in the past but today's society are doing things differently because language today serves the purpose of speed and social interaction." Macquarie Dictionary editorial committee member Sue Butler says grammar and punctuation are increasingly underused in Australia and around the world. "We now do get a failing in standards of punctuation that can be disconcerting," she notes. Media such as television advertisements and public billboards often sacrifice grammar and punctuation to engage audiences in the most efficient, shortest time possible, and correct grammar also is a low priority on live radio and television when politicians and news presenters make mistakes because they have to think and speak faster, says Butler. (The Age 23 Apr 2004, rec'd from John Lamp, Deakin University)

## Category 31.2 Estimates, guesses, predictions, forecasts concerning security 2004-05-19 companies accountable vulnerable software corporations 150 lobbying unsecure Business Roundtable

### NewsScan

### CORPORATE EXECS BLAST TECH INDUSTRY FOR SHODDY PRODUCTS

The Business Roundtable, a trade group for executives of 150 large U.S. corporations, has launched a lobbying campaign to make technology companies accountable for software that they say is vulnerable to hackers and overly complex to use. The group is urging tech firms to improve software design, make software easier to manage, and to continue tech support for software products that have been superseded by newer versions. "Up until now, the IT suppliers have deflected criticism and redirected criticism to end users... We would challenge the software industry to create products that are easier to use, where security is a default component of the software. It shouldn't require somebody with a technology degree to manage a home computer," says a Roundtable spokeswoman. The Roundtable's complaints mirror those made by some consumer groups and security experts, but were met with skepticism by technology representatives. "Cybersecurity is everybody's responsibility, including the vendors, the users, enterprises and government agencies," says a spokesman for the Information Technology Association of America. "No serious commentary will say that the user has no responsibility. We all have responsibilities to lock our doors in our homes and to buckle up when we get in cars." (AP 19 May 2004)

Category 31.2 Estimates, guesses, predictions, forecasts concerning security

2004-08-03

### security spending prediction forecast increase 2005 decrease 2006

DHS IAIP Daily;

http://www.itweb.co.za/sections/business/2004/0408031150.asp ?A=SEC&S=Security&O=FPT

August 03, ITWeb — Security spending to hit high in 2005.

Next year will be the high mark in corporate IT security spending, after which spending will drop to around 5% of IT budgets, says Gartner analyst Rich Mogull. "The reason for this will be because corporations would have to build more secure networks to protect the enterprise," Mogull said at the Gartner Symposium/ITxpo Africa being held in Cape Town this week. According to Gartner's predictions, by 2006, information security spending will drop to 4% or 5% of IT budgets on average as enterprises improve security management and efficiency. The lowest- spending 20% of organizations, the most efficient ones, will safely reduce the share of security in the IT budget to between 3% or 4% in two years. However, Mogull said security managers should include estimates of measurable security improvement with every request for spending. Business units should include security spending in all IT project requests. "The myth that software has to have flaws is only true if you use flawed software," he said. Mogull's list of security technologies that companies will need includes quarantine/containment, security audit capabilities and automated password management. Security technologies that would probably not be needed include personal digital signatures, quantum key exchange, and 500- page security policies.

Category 31.2 Estimates, guesses, predictions, forecasts concerning security

2004-08-30 information technology IT spending survey increase

DHS IAIP Daily;

http://news.com.com/Survey%3A+IT+spending+to+grow+modestly+n ext+year/2100- 1022\_3- 5330227.html

August 30, CNET News.com — Survey: IT spending to grow modestly next year.

IT spending on goods, services and staff is expected to grow 6.4 percent in the United States next year, according to Forrester Research's quarterly survey of chief information officers. That expectation reflects modest growth and an improvement from the past two quarterly polls of CIOs. "Despite the negative perception from oil prices and software vendors putting out quarterly warnings, CIOs are generally expecting a modest growth cycle," said Tom Pohlmann, Forrester research director.

Category 31.2 Estimates, guesses, predictions, forecasts concerning security

### 2004-10-22 predictions robots UN Colin Angle iRobot

NewsScan; http://apnews.excite.com/article/20041022/D85S6N380.html

NUMBER OF DOMESTIC ROBOTS TO INCREASE SEVEN-FOLD

The U.N.'s annual World Robotics Survey predicts that the use of robots for such domestic chores as mowing lawns and vacuuming floors will surge sevenfold by 2007, as the result of steadily dropping prices. Sales of window-washing and poolcleaning robots are also set to take off. Colin Angle of iRobot says, "We are just at a point where robots are becoming affordable... and some of them can actually do real work." The World Robotics Survey predicts that by the end of this decade robots will "also assist old and handicapped people with sophisticated interactive equipment, carry out surgery, inspect pipes and sites that are hazardous to people, fight fire and bombs." (AP 22 Oct 2004)

Category 31.2 Estimates, guesses, predictions, forecasts concerning security

2004-11-01 social engineering information security risk prediction ten years Gamer research

DHS IAIP Daily; http://software.silicon.com/malware/0,3800003100,39125457,00 .htm

November 01, Silicon.com — Social engineering becoming greatest risk.

The greatest security risk facing large companies and individual Internet users over the next 10 years will be the increasingly sophisticated use of social engineering to bypass IT security defenses, according to analyst firm Gartner. Gartner defines social engineering as "the manipulation of people, rather than machines, to successfully breach the security systems of an enterprise or a consumer." This involves criminals persuading a user to click on a link or open an attachment that they probably know they shouldn't. "Criminals are using social engineering to take the identity of someone either for profit, or to gather further information on an enterprise," said Rich Mogull, research director for information security and risk at Gartner.

Category 31.2 Estimates, guesses, predictions, forecasts concerning security

2004-11-19 research development R&D needed information security President committee US PITAC report

DHS IAIP Daily; http://www.gcn.com/vol1\_no1/daily- updates/27979- 1.html

November 19, Government Computer News - More funding needed for security R&D, IT committee says.

The government has shortchanged basic research into cybersecurity and should at least quadruple the money available for civilian research, a subcommittee of the President's IT Advisory Committee (PITAC) said in a draft report presented Friday, November 19. The government plays a key role in supplying the intellectual capital to improve the security of IT systems, said F. Thomas Leighton, chairman of the PITAC subcommittee on cybersecurity. "The government has largely failed in this regard," he said. In addition to being underfunded, government research efforts are becoming increasingly classified and focused on short- term results, the committee found. The subcommittee identified ten critical areas for future research including securing fundamental networking protocols, end- to- end system security, and cyberforensics tools. The subcommittee expects to present a final draft report at the next PITAC meeting on December 5.

### IYIR 2004

Category 31.2 Estimates, guesses, predictions, forecasts concerning security
Calegoliv = 51.2 Estimates, guesses, incurring solution subscription for the second

2004-12-03 information technology IT spending six percent growth 2005 prediction

DHS IAIP Daily;

http://www.computerworld.com/managementtopics/management/its pending/story/0,10801,98040,00.html

December 03, InfoWorld — IT spending to grow six percent in 2005.

In making its annual predictions for the upcoming year, IDC said it expects worldwide IT spending to grow 6.1% for 2005, a year that will be marked by "enormous turbulence" and significant consolidation and realignment in several key sectors. The 6.1% growth, a slight improvement over the 5% growth rate expected for 2004, means the IT market will exceed \$1 trillion in overall spending. What will spur some of this higher growth will be the migration by larger IT shops toward more dynamic IT environments, those that innately offer greater efficiency and better business responsiveness. IDC predicted that there would be a concerted quest for "business value" that will force an increasing number of infrastructure players to partner and acquire technologies and companies that can help them zoom to the upper stack of dynamic IT environments. IDC also predicted the continued rise of open- source software, including the Linux operating system and compatible middleware applications.

# 31.3 New technology with security implications

Category 31.3	New technology with security implications
2004-02-09	Google hacking hobbyist technology uncover sensitive documents information Internet

### NewsScan

### GOOGLE-HACKING TAKES OFF

Google is increasingly becoming a hacking tool for techno-hobbyists who seek out sensitive documents using Google's powerful search capabilities. "There's a whole subculture that's doing this," says Chris O'Ferrell, chief technology officer of security consultancy Netsec, who notes that Google is the search tool of choice for these folks because of its effectiveness. "The reason Google's good is that they give you more information and they give you more tools to search." Companies, organizations and government agencies could block Google from accessing documents by setting up a digital gatekeeper in the form of a robots.txt file that dictates which pages are accessible to Google, but many don't bother, leaving such sensitive information as medical records, bank account numbers, students' grades and the docking locations of 804 U.S. Navy ships, submarines and destroyers open to viewing. Search strings with "xls," or "cc" or "ssn" often bring up spread sheets, credit card and social security numbers linked to a customer list. "It's the easiest point-and-click hacking — it's fun, it's new, quirky and yet you can achieve powerful results," says security consultant Edward Skoudis. "This concept of using a search engine for hacking has been around for awhile, but it's taken off in the last few months." Companies are urged to be more careful about what they put on the Web in the first place, because thanks to caching technology, "Once it is placed online, it's very hard to get the digital horse back in the electronic barn," says Marc Rotenberg, executive director of the Electronic Privacy Information Center. (Washington Post 9 Feb 2004)

Category 31.3 New technology with security implications

### 2004-02-10 VPN virtual private network Georgia state deployment

### DHS IAIP Daily;

http://www.fcw.com/geb/articles/2004/0209/web-georgia-02-10-04.asp

February 10, Federal Computer Week — Georgia to build state VPN.

The Georgia Technology Authority this week released a request for proposals for a new statewide virtual private network (VPN). The new Multiprotocol Label Switching (MPLS) VPN would replace the existing frame relay network used by state, county and municipal government organizations. That includes schools, libraries and law enforcement agencies. It is expected to be cost at least \$10 million). The MPLS VPN will allow administrators to ration and prioritize bandwidth for mission- critical applications. New security and privacy requirements - including federal mandates and common business needs - are also taking agencies beyond the existing network's capabilities. Initially, the network will provide data and video, including videoconferencing for distance learning and telemedicine. The architecture must, however, support the inclusion of voice over IP a year after the initial deployment. One of the biggest advantages to the new network will be the support for mobile workers, allowing users to connect via Digital Subscriber Line, cable modem or dial- up. In addition to standard telework environments, the mobile access will be key for public safety, family and children services site visits, and staff working in state parks.

Category 31.3 New technology with security implications

### 2004-03-01 cell phone security telephone network attack RSA conference

### NIPC/DHS

February 27, Knight Ridder Newswire — Cell phone security.

Computer- security experts say cell phones could be the next carriers for computer- network attacks. Computer- security experts in San Francisco this week at the annual RSA Conference swapped stories about attacks and discussed the possible next big threat. Experts generally agree that 2004 will bring more worms and viruses that can spread among computers with increasing speed. But as computer users grow more savvy about protecting their machines from attack, hackers could turn their focus to the growing number of cell phones and other handheld devices. With more memory and faster processing power than before, these devices are mini- computers, connecting to the Internet and running many of the same programs as desktop machines. But they don't have anywhere near the same levels of protection from cyberattacks. "They are in growing numbers susceptible to the same types of attacks that we've seen on traditional wired machines," said Carey Nachenberg, chief architect with the research labs of the antivirus company Symantec. "The reason why we probably haven't seen any real worms for these platforms is they are not nearly as pervasive as the other platforms. That will change."

Category 3	31.3	New technology with security implications
------------	------	---

2004-03-04 hard disk drive HD heat monitor sensor health lifespan

NewsScan

NEW SENSOR MONITORS HARD DRIVE HEALTH

Researchers at Carnegie Mellon University have developed a new heat-sensitive sensor that can alert computer users to imminent hard drive failure. "Essentially what we are trying to do is save the life of the computer hard drive. Hard drives get hot and the sensor is designed to pick up the slightest temperature variation," says CMU scientist Michael Bigrigg. The researchers predict that by using the dime-sized sensor they may be able to extend the lifespan of a computer hard drive beyond its 3.1 year average by tracking how much daily heat a hard drive endures. (Science Daily 4 Mar 2004)

Category 31.3 New technology with security im	Category 31.3	New technology with security implications
---	---------------	---

### 2004-04-30 bar codes people tracking surveillance school Long Island

DHS IAIP Daily; http://www.gcn.com/vol1\_no1/daily- updates/25816- 1.html

April 30, Government Computer News — Long Island school tests bar codes for emergencies.

An elementary school on Long Island is trying out bar codes as a way to keep track of students during emergency evacuations. Bretton Woods Elementary School in Hauppauge, NY, held a drill on the morning of April 23. Overseen by Hauppauge Schools security director Edward Spear, the faculty evacuated about 800 children onto 16 school buses, which took them to a nearby high school. Stickers with bar codes were placed on the backs of the children's shirts as they left classrooms. When the students stepped off the buses, their bar codes were read by four people holding bar code readers and transmitted to a notebook computer for comparison against an attendance list. Each sticker held a Portable Data File 417 two- dimensional bar code. Although most of the tags were readable without problems, a few proved difficult to scan because they were wrinkled during transit, Spear said. The tags could be placed on identification cards or book bags as an alternative to placing them on clothing.

Category 31.3 New technology with security implications

### 2004-05-17 remote control transportation trains reliance on technology

DHS IAIP Daily; http://jacksonville.com/tu- online/stories/051504/bus\_1561500 2.shtml

May 17, The Times- Union (Jacksonville, FL) — Remote- control locomotives safer, federal report shows.

Switching railcars using remote- control locomotives instead of engineers results in improved safety, according to a preliminary report issued Thursday, May 13, by the Federal Railroad Administration. Such locomotives are increasingly popular with railroads, including CSX Transportation and Florida East Coast Railway, but their use is criticized by the main engineers union, which says they result in increased accidents and injuries. The injury rate of railroad workers in rail yards across the country dropped 57.1 percent with remote- control locomotives, according to the study, which reviewed 2003 data from May 1 through November 30. When the locomotives are equipped with remote control, the engineer's job is eliminated, leaving the train to be run by a two- person team including a conductor equipped with a belt pack. Having fewer employees reduces railroads' labor costs. The Brotherhood of Locomotive Engineers and Trainmen fired back at the positive numbers with a statement saying they were derived solely from data provided by the railroads. It referred to a March AFL- CIO resolution calling for an end to the use of remote- control locomotives. The resolution said that without proper safeguards, it "places all rail workers at risk of injury and death."

```
Category 31.3 New technology with security implications
```

### 2004-07-23 China national technology standards DVD Centrino Windows

NewsScan

CHINA GOES IT ALONE ON HIGH-TECH STANDARDS

DVD? China's trying to do it one better -- with a technology called EVD. CDMA? The digital cell phone standard is so 2003, the Chinese say. Give TD-SCDMA a try instead. Intel's Centrino and Microsoft's Windows? If you're doing business with Beijing, better bone up on WAPI and Red Flag Linux, too. These days, China's dominant message is this: We'll embrace the world -- but on our terms. And nowhere is this more evident than in the realm of high technology, where behind the acronyms is a battle of standards that could have global repercussions. Pushed by their government, Chinese firms are shunning technological protocols invented abroad and developing their own.

They want Chinese-made video discs to run on Chinese-invented players, and they want Chinese consumers linking up with China-developed mobile gadgets. (The Age 23 Jul 2004) Rec'd from John Lamp.

## Category 31.3 New technology with security implications 2004-08-16 new technology PC masses illeterate uneducated developing countries affordable entertainment information

NewsScan

A PC FOR THE MASSES

Carnegie Mellon University professor Raj Reddy is working with researchers at the Indian Institute of Science, the Indian Institute of Information Technology and the University of California Berkeley to develop a low-cost wireless PC designed for users in developing countries, particularly those with large populations who cannot read. The \$250 PCtvt is controlled by a simple TV remote control and can function as a television, DVD player, telephone and videophone. Reddy sees his project not only as a philanthropic effort, but one that may even produce profits. "I kept asking myself, 'what would the device have to do for someone on the other side of the digital divide to be desirable?" The result is a simple device that offers a seductive combination of connectivity and

entertainment. "Entertainment is the killer app, and that will smuggle something that is a lot more sophisticated into the home," says Tom Kalil, special assistant to the chancellor for science and technology at Berkeley. (New York Times 16 Aug 2004)

## Category 31.3 New technology with security implications 2004-11-29 surveillance software SAME see anywhere map anywhere Vincent Tao Canadian inventor

DHS IAIP Daily; http://www.reuters.com/audi/newsArticle.jhtml?type=technolog yNews&storyID=6946893

November 29, Reuters — Canadian inventor lets everyone be an armchair spy.

New Internet- based technology could soon turn regular computer users into armchair spies, a Canadian inventor said on Monday, November 29. Vincent Tao, an engineer at Toronto's York University said he has invented a mapping and surveillance tool called SAME (see anywhere, map anywhere), that produces images so sharp that geographic co- ordinates typed into a Website can reveal the make of a car parked on the street - - the resolution is two feet. Tao said the potential applications are broad, including defense, emergency response and environmental monitoring. He added that the technology could become widely available as early as next year.

23

18

### 31.4 Outsourcing

Category 31.4Outsourcing2004-02-09privacy database disclosure outsourcing security

RISKS

THREE DEGREES OF OUTSOURCING LEADS TO DATA DISCLOSURE

Contributor Ed Ravin writes about a case of disclosure of private information from outsourcing. A programmer ("Dennis") working for a community college posted a full database with confidential information on the Internet in asking for technical help. In a different posting, an anonymous programer warned Dennis about the consequences of posting private informatin. Despite this mild warning, the Dennis posted

Category 31.4 Outsourcing

### outsourcing identity theft risk

DHS IAIP Daily;

2004-05-10

http://www.canada.com/vancouver/vancouversun/news/business/s tory.html?id=b3d19fb5- 4675- 4fad- af8d- a118b3cf4fc6

May 10, Canadian Press — Bank of America plans to hire hundreds in India in outsourcing expansion.

Bank of America Corp. may hire 1,500 people at its subsidiary after it opens in southern India this month, 50 percent more than previously disclosed, and the bank has reserved land that would allow for even more expansion. Late last year, the bank said it eventually expected to have 1,000 people at its Continuum Solutions subsidiary in Hyderabad, but wouldn't give specifics about work intended for the center. Executives with the Charlotte, NC- based financial giant said that Continuum employees will initially work with corporate accounts drawn from London operations and later from the bank's offices worldwide. In the future, Indian workers are likely to work with consumer information. The Indian startup is Bank of America's latest step in moving work abroad, part of a cost- cutting trend called offshoring or foreign outsourcing.

Category 31.4 Outsourcing

### 2004-06-08 Australia outsource Optus India call center

NewsScan

OPTUS OPTS FOR INDIAN CALL CENTERS

Optus, an Australian telecom company controlled by the Singapore government, has joined the ranks of other companies using cheap labor in India for some of its call center operations. However, the company's corporate affairs manager has promised Australians: "Optus will always maintain a call center presence in Australia" Optus has about 4000 call center staff in Australia, and it's unclear how many Australian jobs may be affected by the company's new reliance on Indian call center operators. (The Australian 8 Jun 2004) Rec'd from John Lamp, Deakin U.

Category 31.4 Outsourcing

2004-06-16 Microsoft intention offshore outsourcing high-skilled low-cost foreign vendors

NewsScan

UNION VERSUS MICROSOFT ON OFFSHORING

The Washington Alliance of Technology Workers claims to have identified documents that expose Microsoft's intention to hire low-cost foreign vendors to write its software: "These documents clearly show that as a major software vendor they're looking at the highest skilled, highest trained workers to try to move their work abroad." A Microsoft spokeswoman says the company has long hired outside vendors in India and around the world, but that the company's core technology work will continue to be done in-house: "We're in a cyclical business, so that's part of it. In the work we do,

there are areas of expertise. It makes sense to go to the experts because it's not intellectual property, core technology. We'll continue to do that." The documents in question show that Microsoft paid its U.S. workers \$60 an hour for software developers, \$72 for senior software developers, and \$90 for software architects, whereas for workers in India it paid hourly rates of \$23, \$31 and \$36. (Seattle Times 16 Jun 2004)

## Category 31.4 Outsourcing 2004-07-14 outsourcing fear clamor fading management policy cost cutting India computer software

NewsScan

OUTSOURCING OUTRAGE GOING OUT OF STYLE

The clamor against the outsourcing to India of computer software and back-office services appears to have faded substantially. Infosys chief executive Nandan M. Nilekani says: "The backlash against outsourcing has abated, customer spending is on the rise, and we have redesigned ourselves internally to take advantage of the vast opportunities." According to Sunil Mehta of India's leading software industry trade body: "The debate about outsourcing appears to have moved from an emotional, anecdotal, job-losses plane to a more sober, balanced one about the advantages of globalization of services." Ironically, the antioutsourcing clamor in the U.S. has actually turned out to be good for the outsourcing business. Partha Iyengar, research director for Gartner explains: "The backlash proved a gold mine of freepublicity for Indian outsourcing companies," and the U.S.-based CEO of iGate Global Solutions (operates in Bangalore, India) says: "The backlash issue made outsourcing so mainstream that even my barber was speaking knowledgeably about outsourcing." (New York Times 14 Jul 2004)

### **32.1 Censorship in the USA**

Category 32.1 Censorship in the USA

### Child Online Protection COPA Act review Congress civil liberties ACLU free speech

2004-03-02 NewsScan

SUPREMES TO REVIEW CHILD ONLINE PROTECTION ACT

The Supreme Court will do a new review of the free-speech ramifications of Congress' latest version of the 1998 Child Online Protection ACT (COPA). The Justice Department's position is that "there is a compelling government interest in protecting minors from the effects of material that is not obscene by adult standards but that is nonetheless harmful to minors... Minors today can search the Web as easily as they can change television channels. Thus, in the seclusion of their homes or those of friends, unsupervised minors can, with the click of a mouse, visit one pornographic site after another." The American Civil Liberties Union (ACLU) says the law violates the Constitution's First Amendment guarantee of free speech: "COPA's bludgeon suppresses an enormous amount of speech protected for adults and is unnecessary and ill-tailored to address the government's interest in protecting children from sexually explicit content." (AP/Washington Post 2 Mar 2004)

```
Category 32.1 Censorship in the USA
```

### 2004-03-04 children personal private information not for sale law

NewsScan

SENATORS SEEK TO PUT CHILDREN'S DATA OFF LIMITS

U.S. Senators Ron Wyden (D-Ore.) and Ted Stevens (R-Alaska) have introduced the Children's Listbroker Privacy Act, which would limit the sale of personal data on children under 16 without their parents' consent. The bill is part of a larger package of legislation aimed at helping parents fight back against a deluge of commercial messages aimed at their children. Currently companies spend about \$12 billion annually on marketing to children, often using lists from brokers like the Student Marketing Group that reveal the child's name, address, age, ethnicity, religious affiliation, sports activities, hobbies and family income level. "Many large companies see childhood as a commercial free-fire zone. But some things shouldn't be for sale, and our children's personal information is one of them," says Gary Ruskin, executive director of Commercial Alert. (Wired.com 4 Mar 2004)

Category 32.1 Censorship in the USA

2004-07-13 US governmetn South Dakota library censorship Internet usage teen objectionable material

NewsScan

GOV. REMOVES PART OF S. DAKOTA LIBRARY SITE

South Dakota Governor Mike Rounds has had the teen section of the State Library's Web site shut down because it provided links to material he doesn't believe young people should see. The links to which he found objection included one to a Planned Parenthood site and one to Columbia

University's Go Ask Alice! Rounds said: "As a parent, I would be very disturbed to have my children connecting to any of these Web sites." His position is that state government should not feature links to any advocacy groups and that removal of the links isn't censorship because users can still go directly to those organizations' sites. (AP/13 Jul 2004)

### **32.2 Censorship outside the USA**

Category	32.2	Censorship outside the USA	
----------	------	----------------------------	--

### 2004-03-19 China free speech blogs web logs shut down forbidden content

NewsScan

CHINA SHUTS DOWN 'FORBIDDEN CONTENT' ON BLOGS

China has shut down the Web sites containing blogs (i.e., Web logs or online diaries) "because individual postings contained forbidden content." One site was closed simply for "allowing a letter to be posted that was critical of the government." (AP/USA Today 19 Mar 2004)

Category 32.2	Censorship outside the USA
2004-05-07	8600 unlicensed internet cafes political control china

NewsScan

CHINA SHUTS DOWN 8,600 INTERNET CAFÉS IN 3 MONTHS

Chinese authorities say they have shut down more than 8,600 unlicensed Internet cafés in the last three months in their latest campaign to bring the communication channel under tighter political control. Ostensibly, the crackdown is to protect teenagers from long Internet benders playing combat games and the like. The case of two middle school pupils in Chongqing, who fell asleep on a railway line and were run over on March 31 following a 48-hour interactive gaming session, is being cited. But preventing customers from gaining access to "unhealthy information online" is also a concern behind the drive against unauthorized public Internet venues, which was launched in February and will run until August, says the agency that licenses Internet cafés. Preventing anonymous access to the Internet from cafés has been one prong of Beijing's drive to squelch the Internet's political power for the past 18 months, although the excuse has always been the fire risk and protecting juveniles from abuse. (The Age 7 May 2004) rec'd from John Lamp, Deakin University

Category 32.2 Censorship outside the USA

2004-06-07 chid pornography censorship British Telecom British law Page Not Found

NewsScan

BT SYSTEM FOR BLOCKING CHILD PORN SITES

Using a system called Cleanfeed, British Telecom intends to block its 2.7 million Internet subscribers from reaching child pornography Web sites banned under British law. Attempts to reach the sites will result in a "Page Not Found" error message. Cleanfeed will block sites by filtering out either specific domain names or the unique numeric addresses associated with the Web server hosting the site; it can also block individual pictures on sites. In the U.S., civil liberties groups have fought attempts to force service providers to block access to child porn sites, taking the position that such efforts have the unintended consequence of also blocking thousands of legitimate sites. (AP/Los Angeles Times 7 Jun 2004)

```
Category 32.2 Censorship outside the USA
```

### 2004-06-15 China pornographic site censorship illegal harmful online content

NewsScan

CHINA CRACKS DOWN ON PORNOGRAPHIC SITES

China has shut down five pornographic Web sites in a new campaign that asks people to report "illegal or harmful" online content. In what's shaping up as a tough new plan to control the Internet, Chinese authorities say they've received more than a thousand complaints about pornographic material on Web sites in just the last few days. Last week, China launched net.china.cn, a site called the Illegal and Harmful Content Reporting Center. It follows the introduction of numerous measures to curb online activities in the communist country, which now has about 80 million Internet users. (The Age 15 Jun 2004) Rec'd from John Lamp, Deakin U.

Category 32.2	Censorship outside the USA
2004-06-20	China government mandate self-discipline pact Internet rules

NewsScan

SELF-DISCIPLINE IN CHINA

The Chinese government is asking Internet service providers there to sign a "self-discipline pact" and to exercise patriotic judgment: "The basic principles of self-discipline for the Internet industry are patriotism, observance of the law, fairness and trustworthiness." Observance of the pact will require that Web sites post no information "threatening to the national security, social stability or containing superstitious or erotic content." (AP/Los Angeles Times 20 Jun 2004)

Category 32.2	Censorship outside the USA
2004-07-21	Vietnam censorship Internet pornographic anti government crackdown

NewsScan

VIETNAM STEPS UP CONTROL OF INTERNET

Vietnam has stepped up efforts to control the Internet, instructing Internet service providers to terminate contracts with cybercafes that allow customers to access pornographic or anti-government sites. The directive, issued by Minister of Post and Telecommunications Do Trung Ta, is the latest in a string of measures unveiled in recent months to prevent "bad and poisonous information" being circulated online. This latest regulation requires the communist nation's seven state-owned Internet service providers to disconnect cyber-cafes if they allow clients to access forbidden sites. Café owners are also instructed to monitor their customers' use of the Web for any violations of government regulations, such as distributing viruses and accessing pornographic sites or those that "threaten national security." (The Age 21 Jul 2004) Rec'd from John Lamp

Category 32.2 Censorship outside the L	USA
--	-----

### 2004-07-26 China Internet censorship cleanup block pornography crackdown

NewsScan

CHINA WANTS TO CLEAN UP THE INTERNET

Beijing has blocked 988 overseas Web sites and shut down 67 local ones as part of a nationwide campaign to weed out pornographic content on the Internet. The sites shut down during the July 6-21 special operation included Hong Kong sites, and Google was also inaccessible. So far, the

Chinese capital has arrested 13 people suspected of operating the sites. The police had received 10,660 tips from the public, and the majority of those tips were complaints about inappropriate sexual content on the Internet and complaints about pornographic mobile phone short messages. (The Age 26 Jul 2004) Rec'd from John Lamp

Category 32.2 Censorship outside the USA

### Vietnam Internet monitoring Cyber cops fraud hacking banned information

DHS IAIP Daily;

2004-08-04

http://www.boston.com/business/technology/articles/2004/08/0 4/cyber\_cops\_to\_monitor\_internet\_in\_vietnam/

August 04, Associated Press — Cyber cops to monitor Internet in Vietnam.

A new police unit will start cracking down on Internet criminals next month as communist Vietnam works to maintain control over its growing number of online users. The special unit will focus on crimes such as credit card fraud, hacking, gambling and posting banned information online, the Vietnam News reported Wednesday, August 4. Although the unit will take action against those who post anti- communist messages, it will mainly focus on financial abuses, said Nguyen Tu Quang, director of Hanoi's Technology University Network Security Center, which trained the cyber officers. The cyber police unit will work in collaboration with Internet service providers, universities, banks, former hackers and other security forces, Quang said. About two million of Vietnam's 81 million people access the Web. The number of users is expected to triple by next year, the paper said.

Category 32.2	Censorship outside the USA
2004-08-09	anti pornography measures China censorship underage surfing

NewsScan

### TOP CHINESE SITES LAUNCH ANTI-PORN MEASURES

Popular Chinese web sites Sina.com, Sohu.com and Netease.com are complying with orders to clean up web content to "create a green environment for millions of underage surfers." The official Xinhua news agency says that technical measures had been taken to clean up the sites and web-links, as well as to block pornographic content in their chatrooms and bulletin boards. On the main page of Sina.com on Friday, small sections where pictures of scantily dressed embracing couples are normally posted had disappeared, but were replaced with news about internet crackdown on pornographic content. However, a word search still yielded Web pages containing revealing pictures of women, such as a Sina.com sports website which contained a series of pictures taken from a British tabloid newspaper. (The Age 9 Aug 2004) Rec'd from J Lamp

Category 32.2 Censorship outside the USA

### 2004-11-01 China Internet café censorship

NewsScan; http://www.latimes.com/technology/ats-ap\_technology12nov01

CHINA CLOSES INTERNET CAFES

China has shut down 1,600 Internet cafes and fined operators a total of \$12 million because they allowed children play violent games or commit other violations of the government's policies to clean up Web sites and video games. Investigators have inspected 1.8 million Internet cafes looking for unlicensed operations, has ordered 18,000 of them to "stop operation for rectification" of violations. The country has the world's second-largest population of Internet users after the United States, with 87 million people online. Culture Ministry official Zhang Xinjian says: "Porn, gambling, violence and similar problems have adversely affected the healthy development of the Internet in China." (AP/Los Angeles Times 1 Nov 2004)

Category	32.2	Censorship outside the USA
----------	------	----------------------------

### 2004-11-08 Iran censorship pro-democracy websites

NewsScan;

http://www.nytimes.com/2004/11/08/international/middleeast/08 iran.html?oref=login

IRAN'S CRACKDOWN ON PRO-DEMOCRACY WEB SITES

In the past several months Iran has blocked hundreds of pro-democracy Web sites and arrested such journalists as Mahboubeh Abbas-Gholizadeh and Fereshteh Ghazi, both of whom write about women's issues. But the move to block Web sites has the support of senior cleric Ayatollah Makarem Shirazi, who declared in September that Web sites should be blocked if they "insult sacred concepts of Islam, the Prophet and Imams," or if they publish "harmful and deviated beliefs to promote atheism or promote sinister books." (New York Times 8 Nov 2004)

Category 32.2 Censorship outside the USA

2004-11-09 China censorship video game Taiwan independence political television commercial

NewsScan; http://apnews.excite.com/article/20041209/D86S32RG0.html

DISSIN' CHINA

Law enforcement authorities in China have banned the new British computer game "Football Manager 2005" because it refers to Taiwan as a separate country, contrary to the mainland government's insistence that Taiwan belongs to China. The government is searching for the game online and in computer software markets, cybercafes, and places that sell pirated software. A spokesman for the game's developer, Sports Interactive, says it's working on a Chinese version for release in China that will comply with local requirements: "We will follow the correct submission and approval process within China and look forward to feedback from the Chinese authorities on any modifications that may be required." Last week China also banned a Nike television commercial it says is disrespectful and blasphemous toward Chinese culture. The ad features NBA star LeBron James in a mock video with a kung fu master, two women in traditional Chinese attire, and a pair of dragons. (AP/9 Nov 2004)

### **33.1** Acceptable use policies

Category 33.1 Acceptable use policies

2004-10-25 survey mp3 Australia cost appropriate use office policy bandwidth waste productivity

NewsScan; http://australianit.news.com.au/articles/0

WORK MP3s ARE A \$AU60M PROBLEM

Office workers downloading files to build music and video collections cost Australian businesses \$AU60 million a year, a new survey has found. Exinda Networks, a Melbourne-based supplier of network management and monitoring systems, collated recent data from the Australian Bureau of Statistics and one of the nation's largest private Internet service providers, covering around 10,000 online users. Australian businesses, which spend a total of \$AU450 million a year in Internet costs, were forking out an estimated \$AU4.9 million a month for employees' music and video files, the study found. This was the equivalent of one million MP3 files daily and does not include lost productivity costs. (The Australian 25 Oct 2004)

### **33.2 Spam, spim & spit**

Category 33.2 Spam, spim & spit

2004-01-27 spam history culture documented

NewsScan

THE CULTURE OF SPAM

Who would ever have thought that spam would someday be chic, the subject of an avant-garde show titled "Reimaging the Ordovician Gothic: Fossils from the Golden Age of Spam." The display considers how future historians would view today's culture if all they had to go on was a vast collection of junk e-mail. A classification scheme sorts the spam into such categories as Real Estate, Urgent Messages, Work at Home, Goods and Personal Appearance, and the artists have scrawled representative excerpts from each on the walls of a gallery stairwell and packed suitcases with diet pills, house blueprints and some of the other wares frequently hawked online. Just as paleontologists have a hard time recreating the real Ordovician period, which ended about 443 million years ago, the perceptions about modern culture drawn from spam are quite misleading (and humorous): "Little is known of the physiology of the Ordovician body, but the outward appearance was greatly enhanced by drugs which shaped one to look more like those celebrated in Ordovician PORNOGRAPHY. These pills occasionally took the form of patches and other accessories. It is believed that, for a time, these patches took on significance as ultimately ceremonial jewelry," reads one of the plaques in the show. The display is on view at the Spaceworks Gallery in Manhattan through Feb. 7. (AP 27 Jan 2004)

Category 33.2 Spam, spim & spit

spam expensive Transatlantic Consumer Dialogue junk e-mail

2004-02-03 NewsScan

SPAM ISN'T JUST A PAIN: IT WILL ALSO COST YOU MONEY

A majority of consumers surveyed by the Trans-Atlantic Consumer Dialogue said they are shopping less on the Internet — or not there at all — because they dislike receiving unsolicited junk e-mail. The report says, "It is very clear that the majority of citizens are very troubled by unsolicited commercial e-mails. It is also very clear that bona fide businesses are losing money because the disreputable image of spam is making consumers uneasy about engaging in e-commerce." Marc Rotenberg of the Electronic Privacy Information Center concurs with the report's findings and says: "If you continue at this pace, in five years from now I do not think the Internet will be very popular." Peter Ferguson, chairman of the OECD working group on information security and privacy, explains that most governments now view the Internet as a key to the global economy, and he warns: "Spam has certainly the capacity to interfere with that." (Reuters/Los Angeles Times 3 Feb 2004)

Category 33.2 Spam, spim & spit

### 2004-02-05 spam spammers junk e-mail service names alias inbox random number name generator

NewsScan

WHAT'S IN A NAME?

Ever wonder how spammers come up with all those weird aliases they use to pepper your inbox with unwanted messages? Names like Elfrieda Billman and Beiderbecke P. Sawhorse? One possible source is a Web site run by August Kleimo, who built a random name-generator (www.kleimo.com/rand/name.cfm) using all the surnames from the 1990 U.S. census (free on the Census Bureau's Web site). Kleimo says he gets about 3,000 visitors a day, many of them hunting for unusual names to use for fantasy gaming characters, but admits it's possible that spammers are picking up some ideas from his site also. Other name-generator sites include one by Mike Campbell, a software developer and amateur etymologist. Behind the Name (www.behindthename.com/random.html) allows visitors to generate names in various languages, from Icelandic to classical Greek. Chris Pound, who works in the IT department at Rice University, has written more than 40 name generators, one of which merges names from the worlds of Harry Potter and Dickens (www.ruf.rice.edu/~pound). Security experts say it's difficult to outsmart spammers who use randomly generated names that can slip under the radar of so-called Bayesian filters, which target common words used in spam, like Viagra. A human might detect an obviously fake name, but "a filter can't really see the irony of Tupperware J. Smithington," says ePrivacy Group's chief privacy officer. (New York Times 5 Feb 2004)

2004-02-12	spam volume e-mail Hotmail Microsoft statistics
Category 33.2	Spam, spim & spit

 $http://download.microsoft.com/download/2/e/2/2e2850b8-2747-4394-a5a9-d06b5b9b1a4c/callerid_email.pdf$ 

HOT GRIDDLE FOR SPAM

In Microsoft's "Caller ID for E-Mail: The Next Step to Deterring Spam," the author states, "As of mid-2003, about 83% of the e-mail messages received by Microsoft® Hotmail® on a typical day are spam, unwanted and unsolicited e-mail sent indiscriminately to users. That's around 2.5 billion out of nearly 3 billion messages, and the numbers keep climbing."

Category 33.2	Spam, spim & spit
2004-02-15	spam Website masquerading deception US government Federal Trade Commission FTC

NewsScan

FTC WARNING ABOUT PRIVATE NO-SPAM REGISTRY

The Federal Trade Commission has cautioned computer users not to fall victim a Web site claiming to offer an e-mail version of the federal do-not-call registry. Despite the official-looking appearance of the site's URL, the "Do Not Email Registry" has no affiliation with the U.S. government, and is apparently a scam for collecting e-mail addresses on behalf of spammers. However, the site's operators say their registry serves "legitimate direct marketers" who want to make sure their mailings don't go to spam opponents. The e-mail addresses collected by the registry are made available to bulk mailers in an encrypted form allowing them to check for any overlap with their own mailing lists without seeing the actual addresses. (Washington Post 15 Feb 2004)

Category 33.2 Spam, spim & spit

2004-06-16 bulk junk fax rules rescind Federal Trade Commission business productivity time

NewsScan

MOVE TO RESCIND BURDENSOME JUNK FAX RULES

The chairman of a House subcommittee on telecommunications is introducing a bill to rescind FCC regulations requiring senders of commercial faxes to get prior written approval from recipients. Rep. Fred Upton (R, MI) says his proposed bill is "common-sense regulatory relief" for businesses and associations that have been overburdened with paperwork since the regulations took effect. The bill has been endorsed by the full committee's senior Democrat, John Dingell of Michigan. Newspaper publisher Cheryl Kaechele, testifying on behalf of the National Newspaper Association,

told the subcommittee: "Our typical customers are small businesses. They would far prefer to have us send them information by fax than to spend their precious minutes on the telephone or in personal sales calls." And Walt McDonald of the National Association of Realtors testified that the

inconvenience of requiring written permission from potential clients before sending a fax "would be a giant step backwards in a business where good customer service depends on quick turnaround."

Category 33.2 Spam, spim & spit

### 2004-06-16 spammer anti-spam conversion crusader Internet law obedience

NewsScan

FROM SPAMMER ANTI-SPAM CRUSADER

Sued in March by Yahoo for sending millions of unsolicited commercial messages using Yahoo servers, Canadian spam king Eric Head now says he's renounced spamming and will spend his time drumming in a rock band -- and warning children of the evil possibilities of the Internet: "I urge everyone who is involved in the commercial bulk e-mail business to cease all operations unless and until they are completely compliant with the requirements of the new United States anti-spam laws." (AP/USA Today 16 Jun 2004)

Category 33.2	Spam, spim & spit
2004-07-27	spam survey consumer view purchase bargain

NewsScan

WHO WOULD HAVE GUESSED IT: SOME PEOPLE LIKE SPAM!

A Yahoo survey of Internet users found that one out of five U.S. residents admit to buying products from spammers, and one out of three make some kind of response to spam (such as by asking to removed from the list, by insulting the spammer, etc.). In defense of spam, a 30-year-old

computer-book author in Los Angeles says, "Spam can be useful. One person's spam is another person's bargain." Others seize on occasional deals they find -- a practice strongly discouraged by Laura Atkins, president of the anti-spam organization called SpamCon Foundation, who points out: "These spam-reading consumers are perpetuating the problem." (USA Today 27 Jul 2004)

Category 33.2 Spam, spim & spit

### 2004-08-13 Federal Trade Commission FTC CAN-SPAM spam definition junk unsolicited commercial e-mail

DHS IAIP Daily; http://www.gcn.com/vol1\_no1/daily- updates/26907- 1.html

August 13, Government Computer News — FTC proposes definitions for spam.

The Federal Trade Commission (FTC), as the primary enforcer of the CAN- SPAM Act, was required by Congress to define the criteria for determining the primary purpose of an e- mail. If the primary purpose is commercial, the e- mail is subject to the act. CAN- SPAM, which went into effect January 1, prohibits unsolicited commercial e- mail from using misleading subject lines or phony "from" addresses, and requires them to include a valid postal address and a working e- mail address for opting out of future messages. In a notice of proposed rulemaking published Friday, August 13, in the Federal Register, FTC proposed three criteria for different types of messages. The three proposed criteria are based on a single principle: "Determining the primary purpose to be." FTC is accepting public comment on the proposal through September 13. Electronic comments should be submitted through the online form available at https://secure.commentwork.

Category 33.2 Spam, spim & spit

2004-08-25 spam arrests charges law enforcement trials junk e-mail identity theft scams

NYT http://www.nytimes.com/2004/08/25/technology/25spam.html?th

In late August 2004, dozens of people in the US were arrested and charged with crimes for sending junk e-mail, identity theft and other computer-mediated crimes. Federal and state law enforcement agencies and prosecutors cooperated in a nation-wide sweep. Operation Slam Spam involved support from industry groups such as the Direct Marketing Association and was coordinated by the non-profit National Cyber-Forensics and Training Alliance in Pittsburgh. Analysts commented that if spammers were shut down in the USA, overseas spammers, especially in Russia, would fill in the gap and continue increasing the volume of junk e-mail.

Category 33.2 Spam, spim & spit

### 2004-08-25 spam export US CAN-SPAM Act statistics study survey

NewsScan

U.S. LARGEST EXPORTER OF SPAM

The United States is the largest global source of spam, producing more than two of every five messages, a report by security firm Sophos shows. Sophos found about 43% of all spam originated in the United States. The next largest source was South Korea, with 15%, and China and Hong Kong,

accounting for a combined 12% per cent. The report suggests that a U.S. law known as CAN-SPAM that took effect in January has done little to curb the flood on unwanted messages that some see as a threat to the Internet. Chris Kraft, senior security analyst at Sophos, says the results indicate little

overall change from a similar survey in February for the United States. (The Australian 25 Aug 2004) rec'd from John Lamp, Deakin U.

## Category 33.2 Spam, spim & spit 2004-09-08 anti-spam technology subverted SPF Sender Policy Framework authentication MX Logic Logic

NewsScan

SPAMMERS TAKE ADVANTAGE OF SENDER VERIFICATION PROTOCOL

A new study by MX Logic indicates that about 16% of spam mail senders are using a protocol known as Sender Policy Framework (SPF), which has been touted as a spam-blocking tool, thanks to its sender authentication capabilities. "Authentication (with SPF) by itself is not a spam cure-all.

SPF -- as it relates to having an impact on spam -- will hurt only those who spoof domains. You are still going to need content filtering to see if the message was unsolicited," says MX CTO Scott Chasin. Chasin maintains that SPF is only part of the answer to the spam problem: "SPF is great at

combating fraud such as phishing. Phishing attacks are all about spoofing someone's domain name." Chasin says rather than relying on SPF to cut spam, ISPs should be looking into services that could provide subscribers with some kind of measure of the e-mail sender's reputation by certifying some servers as belonging to "good" e-mail senders. "The e-mail filters could then let through legitimate e-mail. It would be 'guilty until proven innocent,'" says Chasin. (CNet News.com 8 Sep 2004)

Category 33.2 Spam, spim & spit

#### 2004-11-02 politics e-mail spam election campaign Democrats Republicans candidates

NewsScan; http://www.washingtonpost.com/wp-dyn/articles/A18746-

2004Nov2.html

POLITICAL E-MAIL SMACKS OF SPAM

An online survey of 1,000 U.S. Internet users indicates that unsolicited e-mail supporting both the Bush and Kerry presidential campaigns were common in the past few weeks, and about 20% of recipients said the messages may have affected their votes. "The cat's out of the bag," says Anne Bonaparte, president of MailFrontier, which commissioned the study. "E-mail is a powerful communications tool and it has vulnerabilities that are being exploited by people who have a point to make." Engaging in political spam does entail the risk of backlash, however, says Jonah Seiger, cofounder of Connections Media. "Spam is a tactic of snake oil salesmen. I don't see an advantage for a group or a candidate associating themselves with this technique." Meanwhile, Larry Purpuro, president of Republican online consulting group RightClick Strategies disagrees: "In the 2004 election, political e-mail is a tactical nuclear weapon. It is to a large extent under the radar screen, but its ability to target and to penetrate the attention of individuals makes it an extremely effective communications tool." Spam advocating a political position is free speech, protected by the First Amendment, and is not considered illegal under the law. (Washington Post 2 Nov 2004)

Category 33.2 Spam, spim & spit

### 2004-11-05 spam law regulation advertisign CAN-SPAM

Washington Post; MSNBC http://www.msnbc.msn.com/id/6411616/

Microsoft's Steve Ballmer ignited a fuse when he sent out a long letter to millions of recipients advertising his company's products and criticizing Linux.

Anti-spam activists accused the company of using e-mail addresses without permission -- in other words, of spamming. Some lawyers specializing in details of antispam laws in the USA criticized the e-mail for failing to include clear and conspicuous instructions on how to be dropped from the mailing list.

Category 33.2 Spam, spim & spit

### 2004-11-09 SPIT VoIP voice over IP spam Osterman

NewsScan; http://www.usatoday.com/tech/news/2004-11-09-spit\_x.htm

SPITTING MAD AT SPAM

Spam over Internet telephony, known as SPIT, will become commonplace as more people make phone calls over the Internet. Internet researcher Michael Osterman warns that Web-based phone systems attacked by spam will "trash voice-mail systems," and explains: "You can easily delete 100 spam text messages. But try to weed through a voice-mail system filled with 100 unsolicited pitches. That's a pain." Spam is already appearing frequently on instant messages, cell phones, and blogs, and one executive of an Internet service provider admits: "As everything gets connected, there are more ways to spam consumers. Spam is everywhere." (USA Today 9 Nov 2004)

### 33.3 Antispam

Category 33.3 Antispam

### 2004-01-19 phishing SPF senders permitted from DNS e-mail servers authentication anti-spam

RISKS; http://spf.pobox.com/

16ff

23

SPF = "SENDER POLICY FRAMEWORK" OR "SOME PROBLEMS to FACE"?

Andrew Rose posted a note in RISKS alerting readers to a new project called SPF (Sender Policy Framework, <http://spf.pobox.com>) that uses "SPF records" to be published in the domain name system (DNS). E-mail sent with fraudulent headers would be identified because the sender would not match an authorized SMTP server registered in the DNS by means of these records. Rose wrote, "The technical work on SPF is now complete and adoption has started. Several thousand domains have published SPF records including some very large domains such as aol.com. Plugins exist for most of the popular MTAs - the only notable exception being MS Exchange." [MTA = Message Transfer Agent]

In a sharply worded riposte in RISKS 23.18, Markus Fleck-Graffe attacked the whole idea of SPF, pointing to these failings among others:

1) All forwarded e-mail must be rewritten (e.g., mailing lists must destroy the original header to substitute their own authorized domain);

2) Forwarded e-mails require a database of reverse mappings to allow bounce messages to reach the original sender;

3) Spammers will subvert the system by establishing their own SPF-enabled infrastructure using temporary domain names;

4) Worms will use the authentic e-mail addresses of their infected host PCs.

Also in RISKS 23.18, Ian Jackson criticized the SPF group for not using the IETF RFC mechanisms to stimulate discussion and improvements of the proposal but rather, "going for a publicity campaign to `bounce' people into adoption."

In RISKS 23.19, Lawrence Kestenbaum detailed the misery caused by spammers and worms that use his e-mail address in FROM lines, causing thousands of bounce messages to arrive at his address daily. He wrote in exasperation, "The critics of SPF suggest that spammers would simply find or invent other addresses to use. Frankly, I don't care about that, so long as they stopped plastering my personal address on hundreds of thousands of fraudulent and disreputable spam messages and viruses, and clogging my server's net connection with vast piles of misdirected bounces."

In RISKS 23.21, Ben Rosengart recommended doing away with the SRS (Sender Rewriting Scheme) part of SPF, leaving forwarded e-mail with the original header unchanged. Peter da Silva pointed out that "Implementing SPF would do nothing for the people receiving thousands of bounces (myself included). It would simply add another filter that bounced messages back to us because `we' weren't using the right server."

Dmitri Maziuk added to the conversation with the observation that "We know that slapping a band-aid onto implementation to fix deficiencies in design doesn't work and creates more problems...." He wrote, "We already have directory servers, we already have digital signatures. All we need is a way to query Domain Name Service for directory server of a domain, and a standard directory query-response for an e-mail address and associated public crypto key." He also darkly suggested that there would be resistance to this scheme from political forces who actually support spam for their own purposes: "...all "anti-spam" legislations are really there to legalize it. Ergo, all you're going to achieve by implementing SPF, blocklists, blacklists, whatever, is to open yourself to lawsuits from `legal' spammers."

In RISKS 23.23, Jonathan de Boyne Pollard bitterly points out that SPF is a short-term move in an arms race and that it fails to solve the underlying problems of SMTP (which include failure to authenticate message origins). He ends, "perhaps the fact that widespread adoption of SPF will do serious damage to the SMTP mail architecture is a good thing. In the battle against unsolicited bulk mail, we've concentrated upon the wrong problem time after time, with mechanisms that address the wrong thing and that don't address the actual "unsolicited" and "bulk" qualities of undesirable mail. SMTP has become less usable, more patchy, and more balkanised with each new bodge, yet continues to bend and not quite break completely. Perhaps the adoption of SPF will turn out to be the straw that finally breaks the camel's back, and that thus finally forcibly weans us off this bad habit of addressing the wrong problem."

### Category33.3Antispam2004-01-22AOL email caller ID anti spam

NewBits; http://zdnet.com.com/2100-1104\_2-5145065.html http://msnbc.msn.com/id/4028710/ http://www.globetechnology.com/servlet/story/RTGAM.20040122.wadware0122/ BNStory/Technology/

AOL tests caller ID for e-mail

America Online is testing an antispam filter intended to accurately trace the origin of e-mail messages, a move that could bring new accountability to the Net if it proves reliable. The online unit of media giant Time Warner last week implemented SPF, or Sender Permitted From, an emerging authentication protocol for preventing e-mail forgeries, or spoofing. The trial involves the company's 33 million subscribers worldwide and is the first large-scale test for the protocol, which standards groups are considering along with various other e-mail verification proposals.

Category 33.3 Antispam

2004-01-23 Can-Spam Act California law suit ineffective useless stupid pointless legislation

NewsBits; http://www.wired.com/news/business/0,1367,62020,00.html

With This Law, You Can Spam

California lawyers and law enforcement officials continued their assault on the Can- Spam Act Thursday, calling it ineffective and warning attendees at a conference on spam and the law that a solution to the spam scourge is still a distant dream. Signed into law by President Bush on Dec. 16, 2003, the Controlling the Assault of Non-Solicited Pornography and Marketing Act requires e-mail marketers to include legitimate return addresses and opt-out information in all e-mail messages that they send.

Category 33.3 Antispam

### 2004-01-28 FTC adult spam labels Can-Spam Act

NewsBits; http://zdnet.com.com/2100-1104\_2-5149613.html http://www.washingtonpost.com/wp-dyn/articles/A57681-2004Jan28.html

FTC proposes adult spam labels

The Federal Trade Commission on Wednesday proposed a mandatory tag for commercial e-mail that contains pornographic material--a stipulation of the new federal antispam law enacted this month. The FTC, which is charged with enforcing the Can-Spam Act, short for Controlling the Assault of Non-Solicited Pornography and Marketing, proposed a rule that would require senders of adult-related e-mail to include the phrase, "Sexually-Explicit-Content:" in messages. That way, recipients would be able to recognize and easily filter such e-mail before viewing it, according to the FTC and backers of the law.

Category 33.3 Antispam

### 2004-02-02 anti-spam spam countermeasure penny message micropayment Microsoft Yahoo defeat

NewsScan

PENNY A MESSAGE?

Microsoft and Yahoo are giving new life to the debate over whether imposing a small charge on senders of bulk e-mail messages would be the best way to defeat spam. Yahoo executive Brad Garlinghouse says that requiring electronic stamps for e-mail would force mailers to send only those offers a significant number of people might accept. "All of a sudden, spammers can't behave without regard for the Internet providers' or end users' interests." The idea doesn't sit well with everyone. Carnegie Mellon University professor David Farber, who runs a popular e-mail list focused on technology policy, warns: "I suspect the cost of postage will start out small and it will rapidly escalate." But the Internet Service Providers are more receptive to such plans, and Linda Beck of EarthLink says: "Sending large volumes of e-mail involve costs that are paid for by the ISPs and eventually by consumers. Should there be some sort of financial responsibility borne by the originators of these large-volume programs? I think there should." On the other hand, Charles Stiles, the manager of America Online's postmaster department, suggests that the plan simply won't do what it's meant to do, and reminds everyone that "it is the spammers who are the ones with the big pockets." (New York Times 2 Feb 2004)

Category33.3Antispam2004-02-06spam anti-spam lawsuits Penny Black Microsoft			
NewsScan MICROSOFT'S "PENI	INY BLACK" WOULD MAKE SPAMMERS AY A PRICE		
Microsoft's new "Penny Black" research project is named after an 1830s stamp used in Britain that reversed the cost of postage to the sender, rather than the original method of charging the letter recipient — but the Microsoft plan would go the other way, and force the sender of an e-mail to incur some kind of cost. Microsoft also is aiming to raise the cost of sending mass e-mail in other ways: it is suing e-mail marketers in New York and Washington for sending massive e-mailings that that slow down the Internet. (Reuters/Los Angeles Times 6 Feb 2004)			
Category 33.3	Antispam		
2004-02-12 antispam challenge-response keyspace automated retry weakness problem CAPTCHA			
RISKS	23	19	
CHALLENGE/RESPONSE SPAM BLOCKING HAS WEAKNESSES			
Thomas Harrington reported on weak implementation of the challenge-response system (CAPTCHA) designed to identify human beings to prevent spam from reaching Earthlink customers. Seems the system is using only a limited number of images of funny-looking numbers and letters that a person can interpret but a 'bot can't. In addition, the system seems to allow unlimited retries, opening the method to automated attack, especially since the total number "of correct answers is very small, so this would be nowhere near as challenging as a typical dictionary-style attack."			

Category 33.3 Antispam

2004-02-20 anti-spam do-not-spam lists Federal Trade Commission FTC mixed success

NewsScan

DON'T-BOTHER-ME LISTS HAVE MIXED SUCCESS

A poll by the Associated Press has found that three-fourths of the people who signed up for the government's new do-not-call registry received fewer telemarketing calls, but the same poll found that few people noticed any difference in the six weeks since a new federal anti-spamming law took effect. The anti-spam bill encourages the Federal Trade Commission to create a do-not-spam list of e-mail addresses, but FTC officials are doubtful of that approach, because of the decentralized and unregulated nature of the Internet. (San Jose Mercury News 20 Feb 2004)

### Category 33.3 Antispam

### 2004-02-24 e-mail sender authentication Caller ID spoofing spam

http://www.microsoft.com/mscorp/twc/privacy/spam\_callerid.mspx

In February 2004, Microsoft announced the "Caller ID for E-Mail Technical Specification." The Microsoft announcement included the following text:

"Caller ID for E-Mail: The Next Step to Deterring Spam" is the Microsoft draft specification to address the widespread problem of domain spoofing. Domain spoofing refers specifically to the use of someone else's domain name when sending a message, and is part of the larger spoofing problem, the practice of forging the sender's address on e-mail messages.

Caller ID for e-mail would verify that each e-mail message originates from the Internet domain it claims to come from. Eliminating domain spoofing will help legitimate senders protect their domain names and reputations, and help recipients more effectively identify and filter junk e-mail.

• Send your comments. We are circulating this initial technical specification for comment because we believe that your feedback can help make it stronger. Before sending a response, please make sure that you have reviewed and that you agree to the terms and conditions outlined in the specification. Please send your questions, suggestions, and comments to LessSpam@microsoft.com.

• Implement the Caller ID for E-Mail specification. For instructions on how to protect your domain name from spoofing using Caller ID for e-mail, please see "Protecting Domain Names from Spoofing: A Guide for E-Mail Senders."

If you're interested in implementing this specification in software, please review the terms of the Caller ID for E-Mail Implementation License before you begin, as the patent license expands upon the rights that Microsoft would grant you or your organization.

The site includes links for two documents: "Caller ID for E-Mail: The Next Step to Deterring Spam" and "Protecting Domain Names from Spoofing: A Guide for E-Mail Senders" which are both available as PDF documents.

Category 33.3 Antispam

### 2004-03-12 electronic e-mail junk spam anti-spam ISP lawsuit litigation

NIPC/DHS

March 10, Associated Press — ISPs sue over spam e- mails.

Some of the nation's largest Internet providers, in an unusual joint effort, said Wednesday, March 10, they filed six lawsuits against hundreds of people who were accused of sending millions of unwanted e- mails in violation of the new U.S. law against "spam." The legal actions represent the first major industry actions under the "can spam" legislation that went into effect January 1. The lawsuits were filed in federal courts in California, Georgia, Virginia and Washington state. The companies said the defendants include some of the nation's most notorious large- scale spammers. The Internet providers- - collectively with tens of millions of subscribers- - said they shared information, resources and investigative information to identify some of the defendants. Dozens of those named in the lawsuits, however, were identified only as "John Doe" defendants who were accused of e- mailing unwanted pitches for prescription drugs, herbal potions and weight loss plans. The "can spam" legislation requires unsolicited e- mails to include a mechanism so recipients could indicate they did not want future mass mailings. The law also prohibits senders of unsolicited commercial e- mail from disguising their identity by using a false return address or misleading subject line, and it prohibits senders from harvesting addresses off Websites.

## Category33.3Antispam2004-03-15mobile cell phone spam control Federal Communications CommissionNIDC (DUS)

### NIPC/DHS

March 11, Washington Post — FCC sets sights on mobile phone spam.

The Federal Communications Commission (FCC) today took its first steps toward banning spam that targets mobile phones and other wireless devices. The FCC said it will ask the public to submit comments on the best ways to prevent the growth of mobile phone spam, a problem that is still uncommon in the United States though experts agree that it- - along with instant messaging spam- - is getting worse. The commission is required to develop the rules because of a recently enacted federal law that tries to stop the expanding spam problem. Signed into law by President Bush last December, the Can- Spam Act mostly targets e- mail spam but recognizes that cellphones and other wireless devices are prime targets for unsolicited advertising. The law gives the FCC less than a year to draft rules to allow consumers to prevent spammers from contacting them on their wireless devices. The commission also is seeking public comment on whether commercial messages should be clearly labeled and whether mobile phone service providers have to get authorization from their customers before sending them commercial messages.

### Category33.3Antispam2004-03-19spam commerical Websites block AOL privacy strict

NewsScan

SHOULD PEOPLE BE BLOCKED FROM REPLYING TO SPAM?

To defeat spammers, America Online blocks the ability of its members to visit Web sites promoted by bulk e-mailers. Most spammer messages include links that lead to Internet sites, but AOL members who now attempt to visit a blocked Web page receive an error message saying simply that a connection to the page could not be made. The result: less business for spammers. But Washington attorney Paul M. Smith, a specialist in Internet and media law, warns: "There is a service to AOL members by doing this, but there's some trade-off... because some people want to go to those sites." AOL is the first — and so far the only — Internet service provider to cut off access to commerce Web sites advertised by spam. Cindy Cohn of the Electronic Frontier Foundation calls the AOL strategy "paternalistic," even if well-intentioned. (Washington Post 19 Mar 2004)

Category 33.3 Antispam

### 2004-03-22 anti-spam struggle ISPs consumer corporate problem

NewsScan

ISPs STRUGGLE TO FIND FIX FOR SPAM

Unless you've been hibernating the last six months, you know that spam not only is a consumer headache — it's turning into a corporate nightmare. U.S. companies spend an estimated \$1 billion a year in extra security, human resources and lost productivity thanks to this cyber-plague, which comprises anywhere between 50-90% of all e-mail. Despite universal agreement on the problem, major ISPs have not been successful in devising a coordinated approach to fight it, relying instead on lawsuits that at best will be only marginally successful at stemming the flow. Yahoo reportedly is moving toward implementing a DomainKeys system that's used to verify the identity of an e-mail sender, while AOL has recently begun testing a DNS-based system called Sender Policy Framework (SPF). Meanwhile, Microsoft has developed its own system called Caller ID for E-mail and several other efforts, such as the Trusted E-Mail Open Standard, are also available. Experts agree that the balkanization of ISP efforts to deal with spam will delay any final solution, and they're looking to the IETF (Internet Engineering Task Force) to come up with a solution that incorporates the best features of these disparate systems. "Sooner or later, we are going to see what is going to be a compromise proposal that includes elements from the more workable proposals being put forward — DomainKeys and SPF, for example," says the CTO for Outblaze, an e-mail service provider. (CNet News.com 22 Mar 2004)

Category 33.3 Antispam

### 2004-03-30 anti-spam AOL sweepstakes spam victims rewarded

NewsScan

AOL UNVEILS SPAM VICTIM SWEEPSTAKES

America Online is launching a sweepstakes program that will award victims of spam various assets seized from spammers. The top prize is a 2002 Porsche Boxster S, purchased with the proceeds from a lawsuit settled with a spammer — one of five antispam lawsuits that AOL filed in federal court last year. AOL executive VP and general counsel Randall Boe says the company sees the sweepstakes program as a "great way to teach spammers a lesson, and reward our members for their continued use of the 'Report Spam' button." The sweepstakes started at 5:00 a.m. this morning and will run till 11:59 p.m. eastern time on April 8th. Details can be found at AOL.com. (Internet News 30 Mar 2004)

0.5			 	 _	
Category	33.3	Antispam			

2004-04-01 spam unsolicited commercial e-mail law enforcement

NewsScan

EU'S PROBLEMS ENFORCING ANTI-SPAM MEASURES

The European Union has again ordered eight of its members to enact privacy legislation governing spam and cookies. Since the initial warning was sent in November, only Sweden has enacted the legislation, while Belgium, Germany, Greece, France, Luxembourg, the Netherlands, Portugal and Finland have not. The EU inability to enforce its own regulations makes it more difficult to get other countries to join the fight against spam and other undesirable Internet activities. (Los Angeles Times 1 Apr 2004)

Category 33.3	Antispam
2004-04-06	anti-spam laws Australia penalties spamming

NewsScan

AUSTRALIAN JUNK E-MAIL LAWS TAKE EFFECT

Hard-core spammers will be the main target when Australia's communications watchdog begins to enforce anti-spam legislation beginning this Saturday. While penalties of \$1.1 million a day will be reserved for prolific spammers, most complaints about spamming will be treated with a simple phone call, according to the Australian Communications Authority. The ACA's focus will be on compliance, says Anti-Spam team manager Anthony Wing. "We are really targeting, in the first instance, the hard-core spammers. As long as people are trying to comply in the first instance, if we get a complaint it will result in a phone call." Wing says reducing the amount of spam that hits Australia's borders is a "longer program" that requires international co-operation. (The Age 6 Apr 2004)

Category 33.3 Antispam

### 2004-04-08 anti-spam dot mail domain white list certified spam free

NewsScan

ANTI-SPAM GROUP PROMOTES DOT-MAIL DOMAIN

Anti-spam organization Spamhaus is proposing a new "dot-mail" domain that would act as a "white list," guaranteeing that all mail sent from it would be spam-free. Companies with dot-mail addresses would be required to ask e-mail recipients for their permission to send mail as well as a confirmation upon receipt. Spamhaus has offered to review all dot-mail applicants to ensure that they are legitimate, but would charge a hefty fee of \$2,000 to do so. One big uncertainty is whether ICANN will approve the new domain, which is under consideration along with dot-tel, dot-travel and dot-xxx, among others. E-mail marketers have expressed interest in the idea, although there's concern over how it would be managed. "There doesn't seem to be any process built in for how to get yourself one of these dot-mail names if they don't choose to give it to you," says a Direct Marketing Association spokesman. The biggest hurdle, however, will be convincing the major ISPs to go along, says Al DiGuido, CEO of bulk e-mailer Bigfoot Interactive. "This idea is stillborn until that happens. Unless Yahoo, MSN or AOL gets behind them, it's going to be a real uphill battle." (Washington Post 8 Apr 2004)

Category 33.3 Antispam

### 2004-04-14 spam junk e-mail explicit labeling Federal Trade Commission FTC

NewsScan

FTC DEMANDS EXPLICIT LABELING OF EXPLICIT SPAM

If you can't stop them, label them. The Federal Trade Commission is requiring pornspam e-mail messages to have an explicit warning on the subject line so that Internet users can easily filter them out. Beginning the 19th of next month, such messages will have to bear a label reading "SEXUALLY-EXPLICIT:" and the messages themselves will be prohibited from containing graphic material. This new federal standard will supersede state laws requiring such labels as "ADV:ADULT" for pornspam. (Reuters/USA Today 14 Apr 2004)

2004-04-28	anti spam ISPs tackle Yahoo Microsoft AOL
Category 33.3	Antispam

NewsScan

ISP HEAVYWEIGHTS TACKLE SPAM

America Online, Microsoft and Yahoo are joining together in an effort to vanquish spam, and are calling for technical changes in the way that e-mail is routed through cyberspace to make it easier to identify the true sender and content of messages. "We are talking about working on ways to change the dynamics of the e-mail system to make it easier to determine what is fraudulent," says MSN VP Brian Arbogast. The companies say they haven't yet discussed exactly what the standards should be, but have agreed they want to include other competitors in their discussions. "Working together, we will have better information about who are the kingpins that are sending the largest volume of spam to our users," says an AOL spokesman. (New York Times 28 Apr 2003)

Category 33.3 Antispam

2004-04-29 spam spammers criminal charges California junk e-mail illegal CAN-SPAM Act

NewsScan

FOUR SPAMMERS FACE CRIMINAL CHARGES

Four California men face criminal charges for sending millions of junk e-mail messages, becoming the first spammers to be charged under the recently enacted federal CAN-SPAM Act. Christopher Chung, Mark Sadek and Daniel and James Lin are accused of secretly hijacking proxy servers -- systems that relay e-mail from any point on the Internet -- owned by unsuspecting businesses such as Ford Motor Co., Unisys and Amoco, and government agencies, including the Administrative Office of the U.S. Courts and the U.S. Army Information Center. The use of proxy servers is a favorite trick among spammers to disguise their identity. "This has been a problem that's plagued the Net for years, and the fact that corporations and government agencies still have open mail servers is scandalous," says one security consultant. "Somebody dropped the ball." If convicted, the men face up to five years in prison for violating the anti-spam law, as well as up to 20 years for mail fraud for distributing an allegedly fraudulent weight loss skin patch. The group also sent spam mail hawking male organ enlargement pills and Viagra. Terence Berg, the assistant U.S. attorney handling the case, warns that this lawsuit is a harbinger of more to come: "This is just a start. There will be many more prosecutions like this. The government is determined to do something about the flood of spam that is polluting the Internet." (Detroit Free Press/SiliconValley.com 29 Apr 2004)

Category 33.3 Antispam

2004-04-30 US new anti-spam law CAN-SPAM act charge

DHS IAIP Daily; http://www.eweek.com/article2/0,1759,1578981,00.asp

April 30, Associated Press — U.S. Charges four under new anti- spam law.

Federal authorities say they managed to pierce the murky underworld of Internet spam e- mails, filing the first criminal charges under the government's new "can spam" legislation. Court documents in the landmark case in Detroit, MI, describe a nearly inscrutable puzzle of corporate identities, bank accounts and electronic storefronts in one alleged spam operation. At one point, investigators said, packages were sometimes delivered to a restaurant, where a greeter accepted them and passed them along to one defendant. Officials at the Federal Trade Commission told U.S. postal investigators they had received more than 10,000 complaints about unwanted e- mails sent by the defendants. Court records identified the defendants as Daniel J. Lin, James J. Lin, Mark M. Sadek and Christopher Chung of West Bloomfield, MI. They were accused of disguising their identities in hundreds of thousands of sales pitches for fraudulent weight- loss products and delivering e- mails by bouncing messages through unprotected relay computers on the Internet. The "can spam" legislation, which went into effect January 1, requires unsolicited e- mails to include a mechanism so recipients can indicate they do not want future mass mailings.

### Category 33.3 Antispam

### 2004-05-14 spam club fighting forum gatecrash Spamhaus techniques IRC DDoS

DHS IAIP Daily; http://www.theregister.co.uk/2004/05/14/spam\_club/

May 14, The Register — Spam fighters infiltrate spam clubs.

Spam fighters are gaining vital clues in the battle to keep in- boxes clean of junk mail by infiltrating spammer clubs. Online spammer forums like the Pro Bulk Club the Bulk Club and bulkmails.org have been gatecrashed by activists from organizations like Spamhaus. Steve Linford of Spamhaus said spammers know this already but they don't know who amongst their number is working for the other side. In theory invitation to the members- only forums of these sites is only by invitation and only to individuals who have a proven track record in spamming. Apart from playing with the paranoia of spammers, the undercover investigation cast light on the latest spammer techniques. Instead of using open mail relays or unscrupulous hosts, spammers are using compromised machines to get their junk mail out. Viruses such as My- Doom and Bagle surrender the control of infected machines to hackers. This expanding network of infected, zombie machines can be used either for spam distribution or as platforms for DDoS attacks, such as those that many online bookies have suffered in recent months. Trade in machines for DDoS attacks normally happens in more in more anonymous IRC channels but spammers are tapping into the same resource.

Category 33.3 Antispam

### 2004-05-20 **businesses acquisitions spam anti-spam**

DHS IAIP Daily; http://www.technewsworld.com/story/technology/33910.html

May 20, TechNewsWorld — Symantec acquires Brightmail.

Symantec has signed an agreement to acquire Brightmail, a maker of anti- spam technology, in a cash transaction valued at approximately \$370 million. The acquisition, conditional upon customary regulatory approval, is expected to close by early July. It is too early to estimate the impact of intangibles on GAAP results from this transaction. As such, Symantec intends to discuss the impact, if any, on GAAP and non- GAAP results at some point in the future.

### Category 33.3 Antispam

2004-05-31 crime fighting detective spam anti-spam money trail legislation Slam-Spam

NewsScan

DETECTIVES FOLLOW THE MONEY TRAIL TO TACKLE SPAM

It seems like spammers have been working overtime since the federal antispam legislation took effect Jan.1, and the government is now turning away from technical fixes offered by software engineers in favor of private investigators' expertise to boost their efforts to stem the deluge of unsolicited e-mail. In an unusual arrangement, the Direct Marketing Association has paid \$500,000 to hire 15 investigators to work alongside the FBI agents and other government officials in a program known as Project Slam-Spam. The project has built a case against 50 spammers, mostly by

following the money trail and relying on informants. "Spammers are more than willing to rat each other out," says Microsoft investigator Sterling McBride. "The most useful information is who pays for various aspects of the spam operation," says attorney David Bateman, who represents Microsoft

in spam cases. "To spam, you need four or five things -- a hosting service, a domain name, mailing software, mailing lists and so on. Each one you have to purchase from someone." Microsoft has filed 53 civil cases against spammers in the last 15 months, based on the work of its investigation

team. "The real key is trying to figure out how to connect the virtual world" with "someone you can hold responsible for this," says McBride. Once you've nailed that down, "you can use all the tools of a normal investigation." (New York Times 31 May 2004)

Category 33.3 Antispam

### 2004-06-17 Federal Trade Commission FTC do-not-e-mail list fail

NewsScan

FTC SAYS NO TO DO-NOT-E-MAIL LIST

The Federal Trade Commission has decided that a "do not e-mail list" modeled after the popular "do not call list" would be completely ineffective -- and might actually have an effect just the opposite of the one intended (since it could be used by spammers to find legitimate e-mail addresses and send more spam). Senator Charles E. Schumer (D., NY) is critical of the FTC's decision and insists that a do-not-e-mail list "is the best thing we have and they ought to try it." But the FTC points out that Britain's ban of unsolicited e-mail resulted in an increase, rather than a decrease, in the amount of spam sent, and John R. Levine, the chairman of an organization called the Anti-Spam Research Group, says adamantly: "A do-not-spam list of individual addresses is unworkable." (New York Times 16 Jun 2004)

### Category 33.3 Antispam

### 2004-06-22 e-mail service providers unite Internet zombie spam computers

NewsScan

AOL, YAHOO, MSN AND EARTHLINK JOIN TO FIGHT THE ZOMBIES

The country's four largest providers of e-mail service have united in a war to defeat the "zombies" -- personal computers that have been surreptitiously invaded by spammers, who then use them to send spam and other messages without the knowledge of the PC owners. The Anti-Spam

Technical Alliance, which includes AOL, Yahoo, MSN and Earthlink, is urging all Internet providers to police their networks more aggressively and to cut service away from zombie machines. There may be hundreds of thousands of zombie PCs around the world, accounting for as much as 40% of all spam that is generated. (Washington Post 22 Jun 2004)

Category 33.3 Antispam

### 2004-06-24 AOL employee lawsuit spam e-mail address theft

NewsScan

AOL EMPLOYEE BUSTED FOR STEALING E-MAIL ADDRESSES

Jason Smathers, a 24-year-old employee of America Online, has been charged with stealing the e-mail addresses of 92 million AOL customers and selling them to spammers. Under a new federal anti-spam law, he faces the prospect of as many as five years in prison plus a fine of \$250,000. The

stolen information includes not only e-mail addresses but also telephone numbers, ZIP codes and the type of credit card the customers use (though not the actual credit card numbers, which are kept by AOL in a separate database). The company says: "We deeply regret what has taken place and are thoroughly reviewing and strengthening our internal procedures as a result of this investigation and arrest." (New York Times 24 Jun 2004)

Category 33.3 Antispam

### 2004-07-07 United Nations UN spam junk unsolicited e-mail legislation

NewsScan

UN SEEKS SPAM MANDATE

The United Nations aims to bring the international junk email "epidemic" under control within two years by standardizing antispam legislation around the world. Representatives from 60 countries are in Australia attending a meeting hosted by the International Telecommunications

Union (ITU). The goal is to develop examples of anti-spam legislation that governments can adopt to make cross-border cooperation easier. (The Australian 7 Jul 2004) Recd from John Lamp

Category 33.3 Antispam

### 2004-07-20 spam anti-spam lawsuit New York settlement spammer

NewsScan

NEW YORK ACCEPTS \$40K TO SETTLE SPAM CASE

New York has accepted \$40,000 (plus \$10,000 in fees) to settle a lawsuit against a marketer charged with sending unsolicited and deceptive bulk e-mail. New York Attorney General Eliot Spitzer said the marketer, Scott Richter, and his company, OptInRealBig.com, have been held "to a new standard of accountability in their delivery of e-mails. If he does not fulfill these standards, he will find himself back in court, facing greater penalties." Scott Richter's father (who is also his lawyer) says the settlement basically involved a "no harm, no foul" situation from Richter's standpoint, and that the NY attorney general's acceptance of \$50,000 -- after initially talking about \$20 million in damages -- "speaks for itself." Neither Scott Richter nor his company admitted any wrongdoing in the settlement. (AP/San Jose Mercury News 20 Jul 2004)

### Category 33.3 Antispam 2004-08-04 wireless mobile device cell phone spam regulator wrath Federal Communications Commission FCC

DHS IAIP Daily;

http://news.com.com/Wireless+spam+draws+regulators%27+wrath/ 2100- 1028\_3- 5296649.html?tag=nefd.top

August 04, CNET News.com — Wireless spam draws regulators' wrath.

The Federal Communications Commission (FCC) on Wednesday, August 4, said that commercial e- mail messages to cell phones or handheld computers would not be permitted unless the recipient had asked to receive the correspondence in advance. But the FCC's decision not to restrict unsolicited text messages sent through mechanisms like SMS, which stands for short message service, creates a potentially huge regulatory loophole affecting tens of millions of Americans. Wireless providers often charge a few pennies per text message received. Verizon Wireless subscribers exchanged 2.3 billion text messages last quarter, up from 2.1 billion during the previous quarter. Cingular Wireless reported 1.4 billion text messages were sent during its last quarter. The FCC's rules permit mobile providers to register their Internet domain names in a master database that spammers are supposed to honor. That database will include only domain names like attwireless.com and t- mobileusa.com, and not individual e- mail addresses of subscribers.

Category 33.3 Antispam

### 2004-08-04 wireless device spam anti-spam Federal Trade Commission rules

NewsScan

FCC MOVES TO PROTECT WIRELESS DEVICES FROM SPAM

The Federal Communications Commission (FCC) is issuing new rules prohibiting marketers from sending commercial electronic messages to wireless technology users who haven't given them explicit permission to do so. The agency is also urging the industry to develop technologies to prevent spam from overwhelming wireless devices the way it now bedevils the Internet. FCC chairman Michael K. Powell says, "By prohibiting all commercial messages to wireless phones and PDAs absent affirmative consent from the consumer, Americans can now use their wireless devices freely, without being bothered by unwanted and annoying messages." (Washington Post 4 Aug 2004)

### Category 33.3 Antispam

### 2004-08-13 spam anti-spam unsolicited junk unwanted e-mail government OECD Organization Economic Cooperation Development

NewsScan

OECD SETS TWO-YEAR DEADLINE TO CUT SPAM

The OECD said last week it has set up a task force to coordinate the fight by government, business and the public against unsolicited email messages, or spam. It has given the new group two years to study spam and develop a counter strategy. The Organization for Economic Cooperation and Development said in a statement the task force would improve the way work on key aspects of the problem was focused and would improve coordination between various bodies looking at the issue. Key objectives included coordinating international policy, encouraging best practice in industry and business, promoting new technical defenses, informing consumers, and facilitating cross-border law enforcement. (The Age, 13 Aug 2004) rec'd from John Lamp, Deakin U.

## Category 33.3 Antispam 2004-08-19 DNA Chung-Kwei Teiresias algorithm spam identification application 96.56% success Thomas J. Watson Center New York

DHS IAIP Daily; http://www.newscientist.com/news/news.jsp?id=ns99996292

August 19, New Scientist — DNA technique protects against 'evil' e- mails.

A technique originally designed to analyze DNA sequences is the latest weapon in the war against spam. The algorithm, named Chung- Kwei, is based on the Teiresias algorithm, developed by the bioinformatics research group at the Thomas J. Watson Research Center in New York. Instead of chains of characters representing DNA sequences, the research group fed the algorithm 65,000 examples of known spam. Teiresias identified six million recurring patterns in this collection. Each pattern represented a common sequence of letters and numbers that had appeared in more than one unsolicited message. The researchers then ran a collection of known non- spam through the same process, and removed the patterns that occurred in both groups. Incoming e- mail was given a score based on how many spam patterns it had. The Chung- Kwei correctly identified 64,665 of 66,697 test messages as being spam or 96.56 percent. Its rate of misidentifying genuine email as spam was just one in 6000 messages.

### Category 33.3 Antispam

### 2004-08-25 spammers cyber criminals arrest John Ashcroft Attorney General noisy trial

NewsScan

SOME VICTORIES AGAINST SPAMMERS AND OTHER ONLINE CRIMINALS

Attorney General John Ashcroft will announce today that federal and state law enforcement agencies have arrested or charged dozens of people for crimes related to spam, identity theft, online credit card fraud, and other criminal uses of computers and networks. Much of the funding for the

operation came from the Direct Marketing Association, whose former president says: "We felt that the key to the new law was enforcement. We want spammers to realize that spam is not a free game for them and that they face real penalties if they continue." Steve Linford, director of the U.K.-based

anti-spam organization called Spamhaus Project, is cautiously optimistic: "Spammers believe that they will never be caught. If they [law enforcement officials] get 10, 20, 30 well-known spammers, the rest of the spam community will start to notice. Any spammers who can be made to give up because they think the F.B.I. is getting too close is very good for us." On the other hand, Linford fears that a victory in one place just sets up a new challenge somewhere else: "Next year and the year after we are going to see Russia as the main spam problem." (New York Times 25 Aug 2004)

Category 33.3 Antispam

### 2004-09-17 e-mail junk unsolicited spammer arrest hunt search bounty Federal Trade Commission FTC America Online AOL objections

DHS IAIP Daily;

http://www.washingtonpost.com/wp- dyn/articles/A27220- 2004Sep 16.html

September 17, Washington Post — Cash bounties for spammers win limited FTC backing.

The Federal Trade Commission (FTC), on Thursday, September 16, gave limited endorsement to offering cash rewards to people who help track down e- mail spammers, suggesting that such bounties might work but in fewer circumstances than had been pushed by some anti- spam activists. Congress asked the FTC to study two possible techniques as part of the first federal anti- spam law passed late last year. In June, the FTC recommended against the first technique, a do- not- spam registry, saying it would not work and might lead to more spam. The notion of bounties drew particular credence when it was pushed by Lawrence Lessig, a Stanford University law professor and one of the country's foremost thinkers on cyberspace law and policy. But the major Internet providers, who have their own spam- fighting operations, counseled the FTC against the idea. An America Online Inc. spokesperson, Nicholas J. Graham, said the use of bounty hunters can create its own set of legal problems that could complicate prosecutions. The commission estimates that rewards would need to be in the range of \$100,000 to \$250,000, which Congress would need to fund because those amounts are unlikely to be covered by damages won in court.

### Category 33.3 Antispam

2004-11-04 antispam first spam felony conviction junk unsolicited e-mail America Online AOL

#### DHS IAIP Daily;

http://www.washingtonpost.com/wp- dyn/articles/A24546- 2004Nov 4.html?nav=headlines

November 04, Associated Press — Two guilty in first felony spam conviction.

A brother and sister who sent junk e- mail to millions of America Online (AOL) customers were convicted Wednesday, November 3, in the nation's first felony prosecution of Internet spam distributors. Jurors recommended that Jeremy Jaynes, 30, be sentenced to nine years in prison and fined Jessica DeGroot, 28, \$7,500 after convicting them of three counts each of sending e- mails with fraudulent and untraceable routing information. Prosecutor Russell McGuire said Jaynes amassed a net wealth of \$24 million peddling worthless products like a "FedEx refund processor," a "penny stock picker" and an Internet history eraser. Virginia, where AOL is based, prosecuted the case under a law that took effect last year which bars people from sending bulk e- mail that is unsolicited and masks its origin. "Spam is a nuisance to millions of Americans, but it is also a major problem for businesses large and small because the thousands of unwanted e- mails create havoc as they attempt to conduct business," Attorney General Jerry W. Kilgore said.

#### Category 33.3 Antispam

### 2004-11-18 e-mail spam Bill Gates Microsoft volume filtering

NewsScan; http://www.siliconvalley.com/mld/siliconvalley/10213910.htm

BILL GATES GETS MILLION OF E-MAILS A DAY

Think you've got spam? Microsoft chairman Bill Gates "literally receives 4 million pieces of e-mail per day, most of it spam," says CEO Steve Ballmer, who notes that the company uses special technology to filter spam intended for Gates. In addition, there are several Microsoft employees who provide human screening. "Literally, there's a whole department almost that takes care of it." (AP/SiliconValley.com 18 Nov 2004)

## Category 33.3 Antispam 2004-11-30 spam Lycos response flooding bandwidth saturation counterattack information warfare Denning lawsuit screensaver

NewsScan; http://www.usatoday.com/tech/products/2004-11-30-lycos-attack-spam\_x.htm?csp=34

### CYBERSPACE ACTIVISM

The German-based Web portal Lycos Europe is offering a screensaver program that chokes spam servers by flooding them with junk traffic. The company argues that what it's doing is perfectly legal, but former FCC chief technologist David Farber comments: "You don't stop a bad thing by being bad yourself. The idea of somebody coming and hitting you and you hitting back, you both end up very hurt. It just aggravates an already serious problem." And noted computer security expert Dorothy Denning, a professor of defense analysis at the Navy Postgraduate School, points out that cyberspace activism of the kind offered by Lycos Europe is likely to have only minimal impact on spam because "the cost of adding extra bandwidth may be worth the reward" that spammers get from their activities. She adds: "The interesting question is whether or not that company [an anti-spam activist company] might be liable under some law, and would probably be liable, certainly, at least under a lawsuit by the spammers." (AP 30 Nov 2004)

Category 33.3 Antispam

### 2004-12-20 spam judgement federal judge RICO Iowa racketeering damages

NewsScan; http://online.wsj.com/article/0

JUDGE SLAMS SPAMMERS WITH \$1-BILLION JUDGMENT

A federal judge in Iowa has awarded a small ISP more than \$1 billion in damages in what's believed to be the largest judgment ever against spammers. The case was brought by Robert Kramer, whose company provides e-mail service to about 5,000 customers, and who filed suit after his inbound mail servers were jammed with as many as 10 million spam-mails a day in 2000. Citing federal racketeering laws (RICO) and the Iowa Ongoing Criminal Conduct Act, U.S. District Judge Charles R. Wolle ordered AMP Dollar Savings of Mesa, Ariz., to pay \$720 million; Cash Link Systems of Miami, Fla., \$360 million; and TEI Marketing Group, also of Florida, \$140,000. "It's definitely a victory for all of us that open up our e-mail and find lewd and malicious and fraudulent e-mail in our boxes every day," said Kramer, who is unlikely to ever collect on the judgments. (AP/Wall Street Journal 20 Dec 2004)

## Category33.3Antispam2004-12-28America Online AOL report spam decline 2004 legislation CAN SPAM act

DHS IAIP Daily;

http://www.washingtonpost.com/wp- dyn/articles/A30433- 2004Dec 27.html

December 28, Washington Post — America Online reports decline in spam in the past year.

America Online (AOL) said Monday, December 27, that it has seen a substantial decline in unsolicited e- mails this year, though some anti- spam experts said the company may be the only Internet provider experiencing such a drop- off. The average number of so- called spam e- mails that AOL blocked daily dropped from a peak of 2.4 billion in 2003 to 1.2 billion late this year. AOL credited anti- spam legislation, such as the federal Can- Spam law, as well as its own spam- filtering software tools, for the decline. AOL remains the largest Internet service provider, with 29 million subscribers worldwide. But an anti- spam expert said AOL's apparent success may not mean that the rest of the Internet is seeing fewer bulk e- mail spam. John Levine, chairman of the Anti- Spam Research Group said, "There are a lot of spammers who specialize in AOL" because the company has such a large subscriber base. Levine said some bulk e- mailers may have backed down from assailing AOL subscribers as a result of the company's aggressive legal actions against spammers. Other Internet providers reported that they have not seen much change in the volume of spam traffic on their networks.

#### Authorization, access controls 33.4

Category 33.4 Authorization. access controls

#### 2004-01-14 insider threat industrial espionage Voltaire

NIPC/DHS; http://www.gcn.com/vol1\_no1/daily- updates/24622- 1.html

January 12, Government Computer News — Intelligence community seeks protection from inside threats.

A team of companies is building a tool to help the intelligence community keep tabs behind its firewalls. The Voltaire system will integrate existing technology to identify suspicious activity by insiders with legitimate access to sensitive information. Voltaire is intended to make it easier for agencies to share sensitive and classified information by providing a tool to enforce access policy and prevent misuse. The goal of Voltaire is to detect and stop the kind of activity that FBI turncoat Robert Hanssen got away with for years. Hanssen gathered and sold information about FBI counterintelligence activities by browsing through computer files to which he had access. Although he had no legitimate need to see much of the information, investigators found he was able to access it over a period of years without raising any flags. A demonstration version of Voltaire is expected to be ready for testing by summer. Feedback from intelligence agencies will then be implemented into a final product.

#### Category 33.4 Authorization, access controls 2004-01-26 NIST IT security draft report guidelines safeguards standards advice risk management

#### DHS/IAIP Update

January 23, Federal Computer Week — NIST releases telnet, IT security drafts.

Federal agencies desiring to minimize work disruptions from outside intrusions can begin with simple safeguards, such as preventing unauthorized users from using the telnet protocol to gain access to a server, according to officials at the National Institute of Standards and Technology (NIST). Draft documents on computer security released Thursday, January 22, by the NIST give an example of how unauthorized telnet users simply identify themselves as a guest to gain access to sensitive government files. The Risk Management Guide for Information Technology Systems suggests that disabling telnet is about a 10- hour procedure. Practical advice in the 58- page document includes other ways that agencies can develop standards for safeguarding sensitive but unclassified information in federal computer systems. As applied to information systems, the guide says, risk management is a responsibility of executive managers to be shared with technical managers, and not a technical manager's sole responsibility. Engineering Principles for Information Technology Security, a 33- page document also released this week, offers an overview of accepted principles and practices for security information technology systems. Additional information can be found on the NIST Website:

http://csrc.nist.gov/publications/drafts.html

## 34.1 Net filters

Category 34.1 Net filters

#### 2004-02-24 pornography indecendy automated filtering false positives failure

RISKS; http://www.mercurynews.com/mld/mercurynews/business/8026783.htm

20

23

SENDING E-MAIL CAN BE A STRUGGLE IF YOUR NAME HAS A 4- LETTER WORD

Drew Dean summarized a story in the \_San Jose Mercury News\_ by Mike Cassidy: >A Scottish gentleman named Craig C\*ckburn (generally pronounced Coburn) had all too difficult a time receiving his e-mail. It turns out that Mr. C\*ckburn's job title is "senior IT application speci\*list", which also has problems due to the word "speci\*list" containing the substring "ci\*lis" (when used as a proper noun, a Vi\*gra competitor). Not new, but increasingly painful for many people.<

Category 34.1 Net filters

#### 2004-05-27 movie censorship filtering DVD player

http://www.nytimes.com/2004/05/27/technology/circuits/27stat.html?ex=140099 0400&en=7f1caf6facfff153&ei=5007&partner=USERLAND

#### AUTOMATED CENSORSHIP

The RCA DRC232N DVD player includes ClearPlay technology that blocks out violence, sexual language, nudity, crude language, cursing, profanity, ethnic slurs, references to drug use and "vain or irreverent reference to G-d or a deity" — automatically. The scene-skipping software is based on profiles downloaded to the player; the profiles are defined by the human operators at ClearPlay. Investigation of the pattern of censorship reveals that the standards of the censors are "wildly inconsistent" (in the words of the New York Times' David Pogue). Pogue points out that "ClearPlay's most ridiculous assumption, however, is that excising only the split second of central violence somehow makes the overall scene less traumatic." In general, reports Pogue, the system seems remarkably tolerant of violence, for all its claims to transform movies for family viewing.

## 35.1 Cybersquatting

Category 35.1 Cybersquatting

#### DNS squatting Kerry Edwards Websie 2004 Presidential election race

2004-07-07 NewsScan

KERRY EDWARDS: THAT'S A FELLOW IN INDIANAPOLIS

Indianapolis native Kerry Edwards, a 34-year-old bail bondsman, owns the Kerryedwards.com domain, but is willing to sell the name -- for the right price. A Kerry spokesman says: "Our campaign did inquire about KerryEdwards.com, but because of the money they were asking for, we took a pass." Kerry Edwards wanted a five-figure payment. A number of other obvious choices for a campaign Web site (including KerryEdwards04.com, KerryEdwards2004.com, and KerryEdwards-2004.com) are already registered. (Washington Post 7 Jul 2004)

## **35.2 Trademarks vs DNS**

Category 35.2 Trademarks vs DNS

#### domain name lawsuit conflict settlement intellectual property

2004-04-21 NewsScan

SEX.COM SAGA CONCLUDES

The lengthy legal battle over the rightful ownership of the "sex.com" domain name has come to a conclusion with VeriSign's agreement to settle for terms that are rumored to be around \$10 million. "This shows that the small guy can eventually beat a huge company. Hopefully, this leads to better care, custody and control over people's intellectual property," says Gary Kremen, who originally registered the name but found in 1995 that Network Solutions had turned the rights over to convicted forger Stephen Michael Cohen, who duped the Internet registrar into believing he had purchased it from Kremen. A federal court in 2001 ordered Cohen to pay Kremen \$65 million, but Cohen skipped the country and is rumored to be living in Monte Carlo. Kremen then set his sights on VeriSign, which had purchased Network Solutions in 2000 and refused to admit any mistake had been made. The company is embroiled in nine other lawsuits over problems with domain-name registrations, according to the company's most recent annual filing with the SEC. (Los Angeles Times 21 Apr 2004)

## **35.3 Politics of the DNS**

Category 35.3 Politics of the DNS

#### Verisign ICANN lawsuit Internet domain SiteFinder website redirection

2004-02-26 NewsScan

VERISIGN SUES ICANN

VeriSign has filed a federal lawsuit against ICANN, the regulatory body, charging that ICANN has unfairly prevented VeriSign from developing new services for Internet users. According to the suit, ICANN "has overstepped its authority by trying to become the regulator of the Internet." ICANN (the Internet Corporation for Assigned Names and Numbers) is a nongovernmental organization empowered by an agreement with the U.S. government, whereas VeriSign is a private-sector corporation. The lawsuit alleges that ICANN improperly prevented the company from maintaining an online search service, 'SiteFinder', that redirected mis-typed Internet addresses to an advertising-supported search service operated by VeriSign. A VeriSign executive said that ICANN had no authority to force it to shut down Site Finder, and complains: "Working the ICANN process is like being nibbled to death by ducks." But critics of VeriSign say that SiteFinder, by redirecting attempts to access non-existent Web sites, would force the rewriting of hundreds of programs and devices across the Internet. (Washington Post 26 Feb 2004)

Category	35.3	Politics of the DNS
----------	------	---------------------

2004-03-11 Internet Corporation for Assigned Names and Numbers ICANN addresses mobile phone manufacturers protocols

NewsScan

SPECIAL INTERNET ADDRESS PROPOSED FOR MOBILE DEVICES

Nokia, Vodafone, Microsoft, Hewlett-Packard and five other companies are proposing creation of a new Internet domain for mobile Web access, probably with a name such as .mobile or .phone. Wireless ApplicaTion Protocol, a protocol created to reformat Web pages for handheld devices, has been submitted to the Internet Corporation for Assigned Names and Numbers (ICANN); it calls for a new for-profit joint venture set up by the companies to manage the mobile registry. A Vodafone spokesman says that a special site for mobile devices "could be organized for speed of download, ease of use and simplicity." (New York Times 11 Mar 2004)

Category 35.3	Politics of the DNS
2004-03-11	Internet Corporation for Assigned Names and Numbers ICANN addresses mobile phone manufacturers protocols

NewsScan

WANTED: INTERNET DOMAIN FOR MOBILE SERVICES

Microsoft, Nokia, Vodafone, Samsung, Hewlett-Packard and Sun Microsystems are proposing a new Internet domain name such as ".mobile" that would be dedicated to online services available to cell phone users. The companies have submitted their request to ICANN, which is soliciting suggestions for new domains before its March 16 deadline. Decisions could be made as early as this year on adding new domain names to the 250 already in existence. (AP 11 Mar 2004)

Category 35.3 Politics of the DNS

#### 2004-03-12 Internet Corporation Assigned Names Numbers ICANN domain wireless registry

NIPC/DHS

March 10, International Herald Tribune — New domain is proposed.

Nine technology and telecommunications companies joined Wednesday, March 10, to announce their application for a mobile- specific domain. The application, submitted to the Internet Corporation for Assigned Names and Numbers (ICANN) the overseer of the Internet's address system, calls for a new, for- profit joint venture set up by the companies to manage the mobile registry. Names purchased from the company would explicitly point to wireless- focused domains, making the registry a new type of electronic postal code on the Internet. The companies could require any name registered under the new address heading to have a mobile- specific purpose. By contrast, names registered for use with .com, .net and other generic endings need not have any specific thematic purpose. After ICANN's current application round closes on March 16, independent evaluators will examine the proposals. The technology and telecommunications group expects the application process to take three to six months, and services based on the new address, if approved, might arrive by the first half of 2005.

Category 35.3 Politics of the DNS

#### 2004-03-24 Internet domain name sale 100 years

#### NewsScan

DEAL OF THE CENTURY — 100-YEAR DOMAIN SERVICE

Responding to frustration over the current Internet domain name registration renewal process, Network Solutions says it will offer a 100-year registration option for \$1,000 per name. "We've had a number of customers who have allowed high-value domain names to lapse," says Network Solutions CEO Champ Mitchell, citing Microsoft's failure to renew its Passport.com address in 1999 and the Washington Post's temporary lapse in renewing its washpost.com domain name earlier this year. Mitchell agreed that most domain owners won't want to pony up \$1,000 for something that costs \$40 per year, but predicted that there might be up to 10,000 potential takers for the 100-Year Domain Service. But Wayne State University law professor Jonathan Weinberg says the deal may not be a bargain for customers. "Just as you wouldn't want to be locked into your phone company for the next hundred years, even if they offered you a really good deal on a phone, it doesn't make a lot of sense to be locked in with a domain registration company for the next hundred years. If Network Solutions should go bankrupt 30 years from now, you're up a creek." (Washington Post 24 Mar 2004)

Category 35.3 Politics of the DNS

#### 2004-10-25 .net domain VeriSign ICANN e-commerce e-mail

NewsScan; http://www.washingtonpost.com/wp-dyn/articles/A60758-2004Oct25.html

'.NET' UP FOR GRABS '

.Net,' the world's fourth largest Internet domain, is looking for a new operator, and experts say the stakes are high. The winner, to be chosen by ICANN, could earn as much as \$30 million a year, but if the domain were to fail, huge e-mail networks like those operated by Comcast and Earthlink, would go down with it. "It's the most important decision ICANN has ever had to make," says Tom Galvin, VP of government relations for VeriSign, which has operated the .net domain up until now. About 30% of all e-commerce traffic and more than 150 billion e-mail messages a year travel through .net. The handover is the culmination of a deal that VeriSign cut back in 2001, when it agreed to relinquish control over .net in favor of near-permanent ownership of the more lucrative .com domain. VeriSign is permitted to bid on the new .net contract, but will not be given preferential treatment. One likely rival will be Dublin-based Afilias, which in 2003 took over technical management of the .org domain. "There's no question that .net helps underpin the Internet," says Afilias CTO Ram Mohan. "The one [assertion] that strikes me as incongruous is that if you touch .net, everything will fall apart." (Washington Post 25 Oct 2004)

Category 35.3 Politics of the DNS

#### 2004-10-28 web domains ICANN .post .travel

NewsScan; http://apnews.excite.com/article/20041028/D860EHTG0.html

NEW WEB DOMAINS ON THE WAY

Two new Internet domain names -- ".post" and ".travel" -- have received preliminary approval from ICANN, which says they could be in use as early as next year. Talks are now scheduled to hammer out the details on creating and running the domain names, a process that could take months. ICANN is also considering proposals for additional domains, including ".asia," ".jobs," and ".xxx," but the oversight group said the .post and .travel names were different from most existing names because they would be set aside for specific industries and interest groups. The Universal Postal Union in Switzerland wants .post for national postal services, local post offices, business partners and stamp collectors. Private delivery services such as FedEx and UPS would also be eligible. The UPU envisions establishing up to 650,000 virtual post offices to enable users to access their local postal functions anywhere in the world. The Travel Partnership Corp., a New York trade group, wants to make .travel available to travel agents, hotels, airlines, B&B operators, tourism bureaus and others in the travel industry. It hopes that having a specific domain will encourage more travelrelated businesses to put their information on the Web. (AP 28 Oct 2004)

#### Category 35.3 Politics of the DNS

2004-11-10 domain hijacking ICANN deadline default transfer contact address errors

NewsScan; http://theage.com.au/articles/2004/11/10/1100021855873.html

NEW DOMAIN RULES 'WILL MAKE HIJACKING EASIER'

New rules for domain transfers will come into effect on Friday, making it easier for people to hijack domains, according to the security and network services company Netcraft. The new rules, set by the Internet Corporation for Assigned Names and Numbers (ICANN), will mean that requests for transferring a domain will be automatically approved in five days unless they are denied by the owner of the domain. Currently, the ownership of a domain and the nameservers allotted are not altered if a request for a transfer evokes no response. Domain owners who do not manage their records carefully face problems under the new regime. If the contact addresses given in the records are incorrect, then a request for transfer would go to a wrong address and after five days of no response, the transfer would become effective. (The Age 10 Nov 2004)

Category 35.3 Politics of the DNS

#### 2004-12-13 ICANN .mobi .jobs domains

NewsScan; http://www.washingtonpost.com/wp-dyn/articles/A61424-2004Dec13.html

ICANN GIVES THE NOD TO TWO MORE DOMAINS

ICANN, the Internet's oversight agency, has given preliminary approval for two additional domain names -- ".mobi," which would delineate Web sites and other services specifically geared toward cell phones, and ".jobs," which would target the human resources community. In October, ICANN gave preliminary approval to ".post" for postal services and ".travel" for the travel industry. ICANN will now begin negotiations with the applicants of all four suffixes on creating and running the domains. There are currently about 250 domain names, mostly for specific countries, such as ".ch" for Switzerland. (AP/Washington Post 13 Dec 2004)

## **37.3 Undergraduate degrees**

Category 37.3 Undergraduate degrees

### 2004-01-16 virus writing class students professor university publicity consortia industry protest ethics education

http://chronicle.com/free/v50/i19/19a03301.htm

COLLEGE COURSE USES VIRUS-WRITING AS TOOL

A storm of criticism washed over a University of Calgary Professor in early summer of 2003 when he announced his intention to teach a fall course entitled "Computer Science 599.48: Computer Viruses and Malware." Assistant Professor John Aycock shocked the antivirus world by including his intention to have his undergraduate students write some malicious code. Many experts objected on the following grounds:

\* Writing malicious code was unnecessary in teaching how viruses, worms and Trojan horses work or how to fight them;

\* Keeping the malicious code contained within the class of laboratory would be difficult or impossible;

\* Some students would take the wrong message home about the ethical implications of creating malicious code;

\* Students with experience writing malware would be on unemployable by antivirus firms, always concerned about the widespread rumor that they engage in writing viruses for profit.

Supporters of the course scoffed at these arguments, assuring critics that the Laboratory would be well secured and insisting on the pedagogical value of such exercises. In addition, they stressed that virus writing would be only a small part of the course, which would also teach students about the history of malware, economic consequences of these programs, countermeasures, legal and ethical considerations, and wider principles of computer and network security.

After the course was over, there appeared to have been no breaches of security and University spokespersons insisted that they would offer the course again despite their critics.

## Category 37.3 Undergraduate degrees 2004-05-13 Norwich University bachelor science computer security information assurance undergraduate

http://www.nwfusion.com/newsletters/sec/2004/0510sec2.html

Bachelor's Program in Information Assurance

by M. E. Kabay, PhD, CISSP Associate Professor, Computer Information Systems Norwich University, Northfield VT

Norwich University is proud to present a completely new Bachelor of Science in Computer Security and Information Assurance (BSIA for short). The program has been designed from the bottom up; unlike most IA undergraduate degrees, it is not an addon to a computer science degree. Instead, the BSIA has been built to include a wide range of interdisciplinary studies that will contribute to a sound management approach to information assurance.

As part of the team that designed the program and as the program director, I was particularly concerned to complement the many find programs already in existence that focus on highly technical aspects of information assurance. Because Norwich is a small school, our division (of Business and Management) decided to emphasize our strengths. The program, unusually for IA undergraduate degrees, includes such topics as criminal law, psychology (especially social psychology), management, finance, statistics, operations management, humanities courses and technical writing as well as the expected mathematics, programming, data structures, databases, systems engineering, cryptography, and networking. There's also room for such courses as computer forensics and special research projects.

While we wait for information to be posted on our University Web site about the new BSIA and also about the revised minor in information assurance programs, I have prepared documentation and placed it online at

http://www2.norwich.edu/mkabay/bsia

On that page you will find the following documents:

\* Short description of the BSIA (Major)

This one-page summary describes why you might be interested in registering for the Bachelor of Science in Computer Security and Information Assurance at Norwich University. HTM PDF

\* Summary of Courses in BSIA (Major)

This one-page sheet lists all the required courses and available options in the BSIA program. HTM PDF

\* Complete Rationale Justifying the BSIA

This document was prepared for the Norwich University Curriculum Committee and provides the complete background for the decision to create the BSIA program. Because of the formatting and footnotes, this document is provided only in Acrobat PDF format.

\* Minor in IA

This one-page summary lists the required courses and their prerequisites for the minor in information assurance. HTM PDF

I hope that you and any students you know or counsel will find this information helpful. I'd appreciate your help in making this information known to any young people who are interested in an IA career.

Please inform me of all errors you find on the Web page and in the documents posted there so I can correct them quickly.

Category 37.3 Undergraduate degrees	
-------------------------------------	--

#### 2004-07-12 cyberterrorism battle universities academia courses degrees CyberCorps

NewsScan

BATTLING CYBERTERRORISM

At the University of Tulsa, a program called Cyber Corps has become one of the nation's largest institutions specifically created to combat cyberterrorism. Since September 2001 the corps has grown from six universities to twenty universities. The Tulsa program and similar programs at Carnegie Mellon University, the Naval Postgraduate School, and the State University of New York at Stony Brook have received large new grants from the National Science Foundation. [The leaders at the Naval Postgraduate School are professors Dorothy Denning and Peter Denning, special friends of NewsScan.] (AP/San Jose Mercury News 12 Jul 2004)

2004-07-20	IBM assistance colleges universities course development Java DB2 J2EE technology
Category 37.3	Undergraduate degrees

NewsScan

IBM OFFER OF ASSISTANCE TO UNIVERSITIES

IBM is offering free access to IBM software and course-development assistance to any university interested in broadening its curricula, in a move designed to ensure that computer-science programs will teach students about open-source software such as Linux and Sun's J2EE and Java languages as well as IBM's proprietary DB2 database and WebSphere Internet software. IBM said it was "getting strong signals from schools that they want an alternative to Microsoft"; Kevin Schofield of Microsoft Research University relations admitted generously: "Anyone who focuses on just one technology is doing themselves a disservice." (Wall Street Journal 20 Jul 2004)

Category 37.3 Undergraduate degrees

2004-08-08 computer science engineering major college university academia technology study

NewsScan

DECLINING NUMBERS OF COMPUTER SCIENCE MAJORS

The Computing Research Association says that the number of newly declared computer science and computer engineering majors in the U.S. and Canada fell last year 23% from the year before. The explanation is fairly straightforward: since the dot-com bust a computer science degree no longer seems the key to instant riches. But Peter Lee, an associate dean of computer science at Carnegie Mellon University, is unworried by the falloff in applications: he thinks today's students are often of higher quality, because they're motivated not by money but by love of technology. (USA Today 8 Aug 2004)

Category 37.3 Undergraduate degrees

2004-10-13 National Security Agency NSA information assurance roadmap IA curriculum program colleges

DHS IAIP Daily; http://www.gcn.com/vol1\_no1/daily- updates/27627- 1.html

October 13, Government Computer News — NSA: Global grid will have data assurance.

The National Security Agency (NSA) is revising its two- month- old, 2,200- page information assurance (IA) roadmap for the Defense Department's Global Information Grid (GIG), NSA's Daniel G. Wolf said Thursday, October 13, at the Microsoft Security Summit East in Washington. After incorporating feedback from government and industry, NSA will release a three- phase architectural plan for secure worldwide data sharing among and across military and intelligence agencies over the next two decades. It spells out no specific solutions at this point, but it will ensure that IA is "baked in" by authenticating credentials, security clearances, roles and situational awareness throughout the GIG, he said. NSA has also recruited 59 colleges and universities to set up an IA curriculum and teach safe programming practices. The Homeland Security Department has joined the Defense Department as a joint sponsor of the IA curriculum program.

## 37.5 Doctoral degrees

Category 37.5 Doctoral degrees

#### US universities science engineering doctorates increase NSF 2004

DHS IAIP Daily;

2004-12-13

http://news.com.com/Science%2C+engineering+Ph.D.+numbers+buc k+downturn/2100- 1008\_3- 5489359.html?tag=nefd.top

December 13, CNET News — Science, engineering PhD numbers rise.

U.S. universities awarded 25,258 science and engineering doctorates from July 1, 2002, to June 30, 2003, according to data published this month by the National Science Foundation (NSF). That's a 2.8 percent rise from the 24,571 doctorates awarded the previous year, reversing a downward trend that began after a 1998 peak of 27,278. Production of science and engineering doctorates in the United States is seen by some as vital to the country's technological leadership, given the way fundamental research can translate into new products and even industries. A more recent worry centers on a decline in enrollment of international graduate students in the United States. Foreigners historically have earned a large percentage of technology- related doctorates. According to NSF data, foreign students with temporary visas comprised 55 percent of the 5,265 engineering PhDs last year. Not everyone thinks the number of PhDs awarded is critical to the country's global competitiveness. Some observers argue that the country already has plenty of doctorates and that a drop in foreign students isn't cause for alarm.

## **37.7 Conferences**

Category 37.7 Conferences

2004-05-17 broadband access social implications

DHS IAIP Daily; http://www.itu.int/newsroom/press\_releases/2004/12.html

May 17, ITU Press Release - Global support for information society targets.

Targets set for improving access and connectivity to information and communication technologies (ICT) by 2015 at the first phase of the World Summit on the Information Society (WSIS) have received strong support in a global International Telecommunication Union (ITU) survey. The Summit approved a Declaration of Principles and Plan of Action that set forth a roadmap to bring the benefits of ICT to underserved economies. The Summit was organized by ITU under the patronage of UN Secretary- General Kofi Annan to ensure that social and economic development, which is increasingly driven by ICTs, will result in a more just, prosperous and equitable world. The survey shows overwhelming support for the belief that if the information society is to be one in which all citizens throughout the world can equally access and use information resources for sustainable economic and social development, that cyberspace should be declared a resource to be shared by all for the global public good. This opinion was held by more than 94% of survey respondents.

Category 37.7 Conferences

### 2004-10-12 India US cybersecurity talks New Delhi security conference intellectual property rights laws discussion

DHS IAIP Daily; http://abcnews.go.com/Business/wireStory?id=158551

October 12, Associated Press (India) — India, U.S. experts discuss cybersecurity cooperation.

At a New Delhi security conference, U.S. Under Secretary of Commerce Kenneth Juster urged India to tighten its laws to protect intellectual property rights and ensure that sensitive information stays out of the hands of tech- savvy criminals. Juster said India must protect the privacy of personal and financial data as an increasing number of American companies rely on Indians to handle their technical operations and other software work. He cited Europe's efforts as a good example.

Category 37.7 Conferences

#### hacker technology fair Italy security privacy implications

DHS IAIP Daily;

2004-10-21

http://www.reuters.com/audi/newsArticle.jhtml?type=technologyNews&storyID=6572719

October 21, Reuters (Milan, Italy) — Beat hackers and learn to spy at Italy tech fair.

Fingerprint sensors, gadgets to pry open doors and transmitters to spy on unsuspecting targets were among the wizardry on show at the opening of Italy's biggest technology fair on Thursday, October 21. This year a large chunk of the fair was devoted to security in its forms reflecting a growing fear of crime and militant attacks. One of the most popular exhibitors was a company called Global System from the tiny city- state of San Marino teaching people how to spy. Global System offers clients tools to pick locks as well as micro transmitters hidden in watches, baseball caps and phones.

## **37.8 Web sites**

Category 37.8 Web sites

#### government Websites Web content posting schedule

DHS IAIP Daily;

2004-05-25

http://fcw.com/fcw/articles/2004/0524/web- web- 05- 25- 04.asp

May 25, Federal Computer Week — Agencies to inventory Web info.

By the end of the year, agencies are expected to have an inventory and posting schedule for information they plan to publish online. The requirement is part of draft recommendations released in April by the Web Content Standards Working Group of the Interagency Committee of Government Information (ICGI), which outlines standards for common information that should be on all federal Web sites to make them more user- friendly. By December, agency officials must make the schedules available for public comment, said Sheila Campbell, co- chairwoman of the working group. "We're hoping this guidance gets out soon" to help agency officials to comply with this recommendation, Campbell said at the FedWeb conference in Arlington, Va. "It's going to take a little bit of effort here." By next month, OMB officials expect to recommend ways to establish a public domain directory and policies to improve agencies' repositories for research and development funds, Womer said. By the end of the year, OMB officials hope to recommend standards for categorizing and indexing government information.

## **38.1** Consumer profiling

Category 38.1 Consumer profiling

#### 2004-01-08 terrorism Microsoft Julie Olearcek staples

#### DHS/IAIP Update

Flight Sim enquiry raises terror alert

A mother's enquiry about buying Microsoft Flight Simulator for her ten-year-old son prompted a night-time visit to her home from a state trooper. Julie Olearcek, a USAF Reserve pilot made the enquiry at a Staples store in Massachusetts, home to an earlier bout of hysteria, during the Salem witch trials.

#### Category 38.1 Consumer profiling

2004-02-04 privacy consumer choices preferences log WebFountain IBM buzz reports Internet scouring

#### NewsScan

WHO'S SAYING WHAT TO WHOM: WEBFOUNTAIN KNOWS

Hundreds of computer servers at IBM's Almaden Research Center in San Jose, CA, each week gathers 250 million new Web pages and the data (512,000 gigabytes of it) to software called WebFountain designed to capture what everybody is saying about something. IBM has begun licensing the WebFountain technology to corporations to create "buzz reports" developed by scouring every part of the Internet (Web logs, chat rooms, newspaper stories, and so forth) to find out consumer reaction to some new product. In contrast to standard search engines that just match patterns, WebFountain takes a subject and does detailed analyses of what it finds, taking special note of how often someone's name is associated with someone else's with reference to a particular topic. (San Jose Mercury News 4 Feb 2004)

Category 38.1 Consumer profiling

#### 2004-05-13 e-mail disk storage advertising profiling

http://www.nytimes.com/2004/05/13/technology/circuits/13stat.html

GMAIL SECURITY ISSUES

When Google announced its new free Gmail service, many people protested in shock at the idea that Google would scan their email messages and introduce tailored advertisements at the bottom of the e-mail. However, as David Pogue of the New York Times pointed out,

\* no human being reads the e-mail;

- \* a file-storage capacity of 1GB per user will radically change how people use the service
- \* there's a good spell-checker
- \* address book
- \* autocomplete for addresses
- \* ability to specify a different REPLY-TO address
- \* online help
- \* keyboard shortcuts for frequent functions
- \* automatic spam filters
- \* 9 month persistence of the account after the last use.

[MK adds: one suggestion is that the 1GB storage capacity would allow users to store files as a kind of universal flash drive. From a security perspective, one should remember that (a) transfer to the remote Gmail server would be unencrypted; (b) any data on that site would, at least in theory, be accessible by Google staff running the servers. I don't think it is likely that this would in practice pose a serious threat, but anyone concerned with critically sensitive data should encrypt them before storing them on the server.]

Category 38.1	Consumer profiling
2004-08-23	radio listening habits tracking privacy concern Navigauge Arbitron

#### NewsScan

#### NEW SERVICE TRACKS CAR RADIO LISTENING HABITS

Wake up, Arbitron -- a new service offered by Navigauge is combining global positioning technology with continuous tracking of the radio dial to measure radio audiences in cars. While Arbitron has long been the dominant audience information supplier, relying on paper diaries filled out by consumer volunteers, Navigauge executives are betting there's room for improvement. "For a long time, the radio industry itself has lamented the fact that it gets a large percentage of consumers' media consumption but a disproportionately small share of advertising revenue," says Navigauge CEO Tim Cobb. "That's based on the fact that they cannot articulate to advertisers the value that they are delivering." Navigauge is hoping that its capacity to track participants cars through GPS technology will add new layers of useful information for marketers. For example, the company will be able to tell marketers where drivers stop for lunch and whether radio commercials change people's destinations or driving habits. The system can also be used to measure the amount of traffic moving past billboards, assisting the outdoor ad industry in determining its signage exposure. (New York times 23 Aug 2004)

Category 38.1 Consumer profiling

#### 2004-10-25 radio monitoring MobilTrak Washington advertising sensing marketing

NewsScan; http://www.washingtonpost.com/wp-dyn/articles/A60013-2004Oct24.html

#### ADVERTISERS TRACK RADIO LISTENING HABITS

In 14 locations around the Washington area, a company called MobilTrak has installed sensing devices on utility poles that pick up the electronic signals from cars' antennas as they speed by and record which station they're listening to. The monitoring process gives businesses a welcome insight into the listening habits of their target audience and helps them decide how to allocate their advertising budget, says MobilTrak managing partner C. David Boice: "It's all about precision marketing. It's about giving marketers real-time data about what's happening in certain areas at certain times so they don't waste their advertising dollars." The most enthusiastic adopters have been car dealerships, who generally believe that 80% of their business comes from people who live or work within 10 miles of their location. One dealer found that the two stations he'd been investing in -- a talkpersonality station and a contemporary music station -- didn't even rank in the top 10 for in-car radio listeners driving by his dealership. "It was a real eye-opener," he says. Currently, MobilTrak picks up only FM signals, but the company says it plans to introduce technology that picks up AM and satellite station signals next spring. (Washington Post 25 Oct 2004)

Category 38.1 Consumer profiling

#### 2004-10-28 fMRI functional magnetic resonance imaging neuromarketing consumer profiling

NewsScan; http://www.siliconvalley.com/mld/siliconvalley/10040162.htm

#### GETTING INSIDE YOUR HEAD

Brain scanning technology (long used to detect conditions such as Alzheimer's and autism) is now being used to understand how people make choices and how they react to such things as religious experiences, Coke versus Pepsi marketing, and Democrat versus Republican political campaigns. Known as functional magnetic resonance imaging (fMRI), brain scans measure blood flow. During an fMRI, active regions of the brain can be seen lighting up on a computer monitor, indicating either empathy or opposition to what (or whom) the subject is being asked to think about. But the technology is raising strong ethical concerns about "neuromarketing" from critics such as Gary Ruskin of the nonprofit organization Commercial Alert: "This is a story of the corruption of medical research. It's a technology that should be used to ease human suffering, not make political propaganda more effective." (AP/San Jose Mercury News 28 Oct 2004)

## Category 38.1 Consumer profiling 2004-10-31 spyware epidemic AOL Microsoft helpdesk support costs performance widespread NewsScan; http://apnews.excite.com/article/20041031/D862JARG0.html

SPYWARE EPIDEMIC THREATENS TO STALL COMPUTER INDUSTRY

Computer makers say that their technical support lines are lit up by consumers frustrated over sluggish performance and increasingly they're tracing the problems back to one culprit: spyware. Companies are concerned about the cost of the calls, but they're even more worried that that customers will wrongly blame them for performance deficiencies. Russ Cooper, senior scientist with TruSecure Corp., says now that spyware has become epidemic, it's time for Microsoft and other technology companies to launch a public education campaign along the lines of the old "Only \*you\* can prevent forest fires" concept. The industry's incentive is pure survival, says Cooper. Microsoft officials blame rogue software for up to a third of applications crashes on Windows XP computers and AOL estimates that just three such programs together cause about 300,000 Internet disconnections per day. Forrester Research analyst Jonathan Penn says spyware-related customer support can cost \$15 to \$45 per phone call, but it's worth it. "Security is a component of loyalty. People, they want all these various services, but they expect security to come with it." (AP 31 Oct 2004)

#### **Trade in personal information** 38.2

Category 38.2 Trade in personal information 2004-01-04 privacy bank account credit card assets stock report information violation 23

RISKS

11

FORGET YOUR BANK BALANCE? IT'S AVAILABLE ON THE INTERNET

Monty Soloman cites an instance of personal financial information being uncovered through Internet asset-research services. The Boston Globe\_was able to discover bank account and stock and bond information of Eric F. Bourassa, a Massachusetts Public Interest Research Group privacy advocate. Bourassa had charged \_The Globe\_ with trying to find as much publiclyavailable financial information about him as possible. An article in \_The Boston Globe\_ about this incident asks where assetresearch firms get their information from: "Does it come directly from financial institutions? Or does it come through more indirect, possibly illegal, methods?"

Category 38.2	Trade in personal information
2004-01-29	technology Internet background checks dating
NewsScan	

SMILE, YOU'RE BEING GOOGLED

By making the mistake of dating a woman who knew how to use the Internet, fugitive LaShawn Pettus-Brown found himself jailed soon after the woman looked his name up in Google and found he was wanted by the FBI for alleged wire fraud. Use of the Internet for background checks is gaining a lot of popularity in the dating world, so stop doing whatever it is you're doing wrong, or restrict yourself to dating Luddites. (USA Today 29 Jan 2004)

Category 38.2 Trade in personal information

2004-03-08 background checks prospective employees product security privacy

NewsScan

BACKGROUND CHECK-IN-A-BOX

ChoicePoint is marketing a new product aimed at security-conscious employers who want to make sure their new hires are trouble-free. Stacked between gallon jars of mayonnaise and office furniture at Sam's Club, the ChoicePoint check-in-a-box package urges shoppers to "make better hiring decisions" by purchasing the \$39.77 product, which contains a CD-ROM that allows users to tap into ChoicePoint's online databases. The new marketing effort signals data vendors' shift toward small businesses, which have lagged behind large corporations in conducting criminal background checks when hiring. Privacy advocates warn that such products put too much information at the fingertips of anyone with \$40 to spend, and argue that ChoicePoint's requirement that users have a business license provides inadequate safeguard against the product's abuse. "If Joe's Bait Shop... goes out and buys this thing with a business license and then he wants to find out information about a neighbor, then he would be able to essentially do that," says the head of the Georgia Association of Professional Private Investigators. (AP 8 Mar 2004)

Trade in personal information Category 38.2

2004-03-19 consumer data sales Australia privacy profiling

NewsScan

SALES OF CUSTOMER DATA RILE AUSTRALIAN TELECOM USERS

Australian telecommunications service providers are selling customer information to other companies for direct marketing and other commercial activities, according to the Australian Communications Authority. Acting ACA chairman Bob Horton cites evidence that customers' information is being collected by producers of public number directories and collated with data from other sources to create consumer "profiles": "Current use of telecommunications customer data appears to go beyond what is allowed under existing legislation. In fact, our investigations indicate that databases are being created and maintained based on information provided by customers to their telecommunications service providers. These databases are then sold to other companies for direct marketing and other commercial activities. In the ACA's opinion, this is not only a breach of existing law but also outside what customers providing personal information expect to happen." (The Age 19 Mar 2004, rec'd from John Lamp, Deakin University)

Category 38.2	Trade in personal information
2004-04-03	Google Gmail e-mail service policy privacy issues

NewsScan

PRIVACY ADVOCATES TARGET GOOGLE'S GMAIL STORAGE POLICY

Privacy advocates are voicing concern over Google's data retention plans, following the search company's splashy launch of its free Gmail service last week. Google's Gmail privacy policy tells users: "The contents of your Gmail account are also stored and maintained on Google servers in order to provide the service. Indeed, residual copies of e-mail may remain on our systems, even after you have deleted them from your mailbox or after the termination of your account." The fact that e-mail records potentially could be combined with Google search cookies, designed to index users' searches through 2038, and an Orkut cookie that contains personal identification information, is what has privacy watchdogs worried. "Once users register for Gmail, Google would be able to make that connection, if it chose to," says Pam Dixon, head of the World Privacy Forum. "And if Google ever compared the two sets of data, there are some people who would be chilled and embarrassed." Archivist Daniel Brandt adds: "While Google brags that no humans will read your e-mails, the entire Gmail program will involve extensive automated profiling of you as an individual. Google will be sharing non-identifiable portions of your profile with anyone they choose. If the ownership of Google changes, or there is a merger, the entire personally-identifiable profile will be available to the new owners or partners." (The Register 3 Apr 2004)

#### Category 38.2 Trade in personal information

#### 2004-05-20 campaign contributions tracking privacy publication access neighborhoods

http://www.nytimes.com/2004/05/20/technology/circuits/20dona.html?th

Fundrace.org provides detailed information on precisely who is giving exactly how much money to which political candidates. The information is public, in that it is registered by the Federal Election Commission and available on demand. However, the shift to Web-accessibility changes the theoretically public into the very public, and not everyone is pleased. Some observers worry about privacy; others about decreasing contributions if everyone's neighbors and employers can check up on political activity.

Category	38.2	Trade in personal information
Cullgory	00.2	i i due in personar information

2004-06-03 data deceased ownership possession

NewsScan

WHO GETS YOUR DATA WHEN YOU DIE?

When a deceased person's family members don't want to go to the time and effort of gaining access to the data on the person's computer, they simply erase the hard drive and get rid of the computer without ever knowing what was on it. The manager of one computer-repair service says, "We're probably wiping away a lot of memories. Most people want to give the computer away without worrying about someone else getting access to personal information. When they bring it in, they don't know what's on it and they don't seem to care." Of course, relatives may also be afraid that there may be e-mail messages or other things on the computer that they'd rather not see. Eric Thompson, founder of AccessData Corporation, suggests that sometimes it might be best to let some secrets go to the grave with the deceased: "When you break into computer files you're reconstructing a person's life, both the good and the bad." (New York Times 3 Jun 2004)

Category 38.2 Trade in personal information

2004-07-07 private customer data privacy Hooked Phonics Federal Trade Commission FTC complaint settlement

NewsScan

#### HOOKED FOR RENTING OUT PRIVATE CUSTOMER DATA

The Hooked on Phonics company, which markets learning systems, has settled a complaint by the Federal Trade Commission that the company rented out customer data to outside marketers even though it had promised on its Web site that it would keep the information private. The FTC's J. Howard Beales III says: "It's simple: If you collect information and promise not to share, you can't share unless the consumer agrees." But Chris Jay Hoofnagle of the Electronic Privacy Information Center criticizes the FTC on the grounds that the Agency is in effect pushing companies to have the fewest restrictions possible without alienating potential customers: "The obvious encouragement here is to not make promises. We think that approach is somewhat inflexible." (Washington Post 7 Jul 2004)

Category 38.2	Trade in personal information
2004-08-31	ACLU American Civil Liberty Union Secret Service Website data sensitive

NewsScan

ACLU DENIES MISCHIEF IN POSTING OF DELEGATE DATA

The Secret Service is investigating the posting on a Web site operated by an organization called the Independent Media Center of the personal information of delegates to the Republication National Convention in New York. The Center describes its activities as "passionate tellings of the

truth." The Secret Service, however, is concerned that posting of the delegate data could subject the delegates to harassment, acts of violence or identity theft. The American Civil Liberties Union is representing the Independent Media Center, and the ACLU's Ann Beeson says: "This type of

investigation is really a form of intimidation and a message to activists that they will pay a price for speaking out. The posting of publicly available information about people who are in the news should not trigger an investigation." (AP/USA Today 31 Aug 2004)

Category 38.2 Trade in personal information

2004-12-21 wireless phone directory assistance Connecticut privacy consumer information

NewsScan; http://www.usatoday.com/tech/wireless/phones/2004-12-21-mobile411\_x.htm

CONTROVERSY OVER WIRELESS PHONE DIRECTORY

Connecticut Attorney General Richard Blumenthal wants the cellular phone industry to discard its plans to create a directory assistance system for wireless phone numbers because there are "too many unknowns and dangers and too few protections at this point." But Kathleen Pierz, a Michigan analyst specializing in directory assistance counseling, says there are plenty of safeguards: "This is so buttoned up from a customer point of view, people don't have to worry. Blumenthal fears that a list of wireless numbers would inevitably be sold to telemarketers: "If the lists are there, they will be sold. They are so valuable. No cell phone company will resist the temptation to sell those lists for the huge profits." Pierz, however, points out that there is no marketing value to such lists because of existing federal laws preventing entities from calling a cell phone. (AP/USA Today 21 Dec 2004)

# 38.3 Industry efforts for privacy protection

Category 38.3 Industry efforts for privacy protection

#### 2004-06-09 Ohio interstate scanning system license plate recognition

NewsScan

OHIO'S TURNPIKE SCANNING SYSTEM

The Ohio State Highway Patrol will be using two scanners on turnpike gates and two scanners in patrol cars for four months, as they test a new system that recognizes license plates and matches them with a national crime database. The scanner company, Elsaq SpA, is based in Genoa, Italy. Jeff

Gamso of the Ohio ACLU worries that the scanners will invade the privacy of ordinary citizens: "It's a free society, and we're supposed to move as we like without the government tracking us everywhere." State Highway Patrol superintendent Paul McClellan says that if the scanners had been in place earlier this year, they might have detected the individual responsible for a number of sniper shootings on state highways. (AP/USA Today 9 Jun 2004)

# **38.4** International agreements on security, privacy, Net law

Category 38.4 International agreements on security, privacy, Net law

#### 2004-02-02 Federal Trade Commission FTC server secure e-mail open proxy spam relay routing

DHS IAIP Daily; http://www.ftc.gov/opa/2004/01/opsecure.htm

February 02, Federal Trade Commission — FTC and international agencies announce "Operation Secure Your Server".

The United States Federal Trade Commission (FTC) and 36 agencies in 26 countries announced "Operation Secure Your Server" on Thursday, January 29, an international effort to reduce the flow of unsolicited commercial e- mail by urging organizations to close "open relays" and "open proxies." As part of the initiative, the participating agencies have identified tens of thousands of owners or operators of potentially open relay or open proxy servers around the world, and the agencies are sending letters urging the owners and operators to protect themselves from becoming unwitting sources of spam. Open relays and open proxies are servers that allow any computer in the world to "bounce" or route e- mail through servers of other organizations, thereby disguising the real origin of the e- mail. Spammers often abuse these servers to flood the Internet with unwanted e- mail. Their abuses not only overload servers, but also could damage an unwitting business' reputation if it appears that the business sent the spam. The FTC and 10 agencies in Albania, Argentina, Australia, Canada, Brazil, Bulgaria, Canada, Chile, Colombia, Denmark, Ecuador, Finland, Hungary, Jamaica, Japan, Lithuania, Norway, Panama, Peru, Romania, Serbia, Singapore, South Korea, Switzerland, Taiwan, and the United Kingdom are sponsoring this initiative.

## 38.5 EU legislation & regulation concerning privacy

Category 38.5	EU legislation & regulation concerning privacy		
2004-01-18	UK data protection act unintended consequences privacy	disclosure	
RISKS; http://news.b	bc.co.uk/1/hi/uk/3395071.stm	23	14

UK DATA PROTECTION LAWS AND THE LAW OF UNINTENDED CONSEQUENCES

Contributor Richard Pennington notes two cases of loss of life resulting from misunderstanding and misapplication of the UK Data Protection Act. In the first case, a school in Cambridgeshire hired an applicant from Humberside for a janitor's job. Background checks with Humberside police had shown the applicant to be 'clean'. Later, this new janitor murdered two schoolchildren. An inquiry showed that the janitor had been investigated in Humberside for indecent assualt. Humberside police stated that they were forced by the UK Data Protection Act to destroy the suspect's records when "investations ended without a trial." So, the suspect's history was not circulated in Humerside, and never reached Cambridgeshire. In the second case, in August 2003, British Gas stopped supplying an elderly couple gas due to bill nonpayment. This couple was discovered to have perished from hypothermia during the winter. British Gas cited the UK Data Protection Act for not contacting local Social Services because "they did not have the written permission of the couple to disclose their financial records." In a follow-up article, the same contributor noted that, at that time, the Data Protection Registrar had been renamed the Information Commissioner. In another follow-up article, contributor Dave Harris, referring to the first case above, said that the killer Ian Huntley had not actually worked at the school where the two children were murdered. Huntley had come "into contact with them through his girlfriend (who did work at their school)."

|--|--|--|

#### 2004-07-01 did-they-read-it e-mail Web bug online service privacy France litigation illegal

NewsScan

#### FRENCH AUTHORITY FORBIDS "DIDTHEYREADIT?" SERVICE

CNIL, the French data protection authority, has declared Rampell Software's new mail-service 'Did they read it?' to be illegal. (Subscribers to "DidTheyReadIt?" get a report about the exact time their e-mail was opened, for how long, on what kind of operating system and if the mail was forwarded to other people.) The CNIL finds the service unacceptable under French privacy Legislation; as a result, any French subscriber to this service risks a prison sentence of 5 years plus a substantial fine. (EDRIgram 1 Jul 2004) Rec'd from Jim Sterne via Mark Gibbs

Category 38.5 EU legislation & regulation concerning privacy

#### data debate privacy Lloyds Britain jurisdiction outsourcing India

2004-08-19 NewsScan

DATA DEBATE STIRS IN BRITAIN

A customer of Lloyds TSB bank has complained to Britain's Information Commissioner arguing that data should not be transferred outside Europe without the consent of individual customers. The complaint by an unidentified Lloyds customer, filed in July, argues that Indian workers would not be subject to the same data protection standards applicable in Europe, according to the Lloyds TSB union, which has been campaigning against outsourcing of work to India and other countries. The Information Commissioner's office said British companies are still bound by European standards when data is transferred overseas: "There are various bases in law which can be used to legitimize the transfer overseas of personal data, consent from the individual is just one of them." (The Australian 19 Aug 2004) Rec'd from J. Lamp

# 38.6 US legislation & regulation concerning privacy

Category 38.6 US legislation & regulation concerning privacy

#### 2004-01-08 email privacy U.S Treasury TTB violation

NewsBits; http://news.com.com/2100-1028\_3-5137488.html

Treasury breaks word on e-mail anonymity

The U.S. Treasury Department plans to publish nearly 10,000 e-mail addresses on the Web, violating its privacy promise to Americans who used e-mail to comment on a government proceeding. In March 2003, the Treasury Department's Alcohol and Tobacco Tax and Trade Bureau (TTB) asked for e-mail comments about a proposal that could raise the price of malt beverages like Bacardi Breezer and Smirnoff Ice. At the time, the department said that the text of comments would be made public--but assured people that e-mail addresses, home addresses and other personal information of individuals would be removed first.

Category 38.6	US legislation & regulation concerning privacy
2004-05-17	privacy protection data mining Donald Rumsfeld Pentagon DoD

NewsScan

PANEL URGES MORE PRIVACY PROTECTIONS IN FEDERAL 'DATA-MINING'

The Technology and Privacy Advisory Committee, a panel created by U.S. Defense Secretary Donald Rumsfeld to scrutinize Pentagon programs in the wake of criticism over the ill-fated "Total/Terrorism Information Awareness" program, is urging Congress to pass laws protecting citizens' civil liberties from overly intrusive federal data mining activities. "The Department of Defense should safeguard the privacy of U.S. persons when using data mining to fight terrorism," says the panel's report, which notes that privacy laws lag far behind current capabilities in information and communications technology. A key recommendation suggests federal agencies should be required to obtain approval from a special federal court "before engaging in data mining with personally identifiable information concerning U.S. persons." Former FCC Chairman Newton Minow, who headed up the panel, acknowledges that the proposals would "impose additional burdens on government officials," but maintains that the requirements would improve national security while enhancing personal privacy: "Good privacy protection in the context of data mining is often consistent with more efficient investigation." (New York Times 17 May 2004)

Category 38.6	US legislation & regulation concerning privacy
2004-06-30	e-mail eavesdropping OK litigation court ruling privacy surveillance law
	enforcement anti-terrorism Homeland Security

NewsScan

COURT RULES E-MAIL EAVESDROPPING OKAY

In a surprise decision, a federal appeals court has ruled that it was acceptable for a company that offered e-mail service to peruse messages sent by its subscribers. The case stems from 1998 when it was discovered that Interloc, a now-defunct literary clearinghouse, surreptitiously copied messages sent to its subscribers by rival Amazon in order to "develop a list of books, learn about competitors and attain a commercial advantage." An Interloc executive was later indicted on an illegal wiretapping charge, but yesterday's ruling upheld a federal judge's dismissal of that charge on the

grounds that the e-mails were copied while in "electronic storage" (during the process of being routed through a network of servers to recipients). The Wiretap Act prohibits unauthorized eavesdropping on messages that are not stored -- such as a real-time telephone conversation -- but does not afford the same protection to stored messages. In a dissenting opinion, Appeals Court Judge Kermit Lipez wrote that the ruling unravels "decades of practice and precedent regarding the scope of the Wiretap Act" and essentially renders the act "irrelevant to the protection of wire and electronic privacy." In a concurring statement, the Electronic Frontier Foundation said that yesterday's ruling "dealt a grave blow to the privacy of Internet communications." (AP 30 Jun 2004)

Category 38.6	US legislation & regulation concerning privacy
2004-08-28	Federal Communications Commission FCC telephone outage information kept

DHS IAIP Daily;

http://www.washingtonpost.com/wp- dyn/articles/A40329- 2004Aug 27.html

August 28, Washington Post — FCC cuts public line to phone outage data.

The Federal Communications Commission (FCC), citing concerns about national security, has abandoned a 10- year- old policy and will no longer give the public access to information about past telephone network outages. The decision has angered consumer advocates and some state regulators who say the data are a critical tool in evaluating phone service reliability around the country. Large companies use the information to make decisions about where they build their own networks and to plan for key facilities such as data centers. While the FCC limited the amount of information it is making public, it has expanded the amount of information it collects from the wireless and satellite industries. Under the new rules, wired, mobile and satellite carriers must report an outage that affects 900,000 user minutes or more. Although the FCC will not make the information it collects about the outages public, the companies are free to keep the public informed about outages as they are occurring.

### Category38.6US legislation & regulation concerning privacy2004-10-01clickwrap agreements tiny print examination study privacy security operability

utility usability legal mumbo-jumbo privacy

NewsScan; http://www.wired.com/wired/archive/12.10/view.html?pg=2

WHAT THE WORLD NEEDS IS MORE LAWYER-BOTS

Mark Rasch, founder and former head of the U.S. Justice Department's computer crimes unit, says that the increasing trend toward lengthy, tiny-font policy "agreements" that users must click on before they can access a Web site are generating the need for more legal oversight. "Increasingly, companies have been putting some pretty nasty things into their clickwrap agreements -- such as that they can collect and sell your detailed personal information or install software that will capture your every keystroke... This is not legal boilerplate, the kind that everybody assents to when renting a car or buying a ticket to a ball game. It affects the privacy, security, and operability of all of the information you access online." Rasch says what's desperately needed is a law robot -- "a browser-based automaton that could be adjusted to match your tolerance for legal mumbo-jumbo... Once you establish privacy settings, your browser would transfer personal data (after prompting you) only to sites that conform with your privacy requirements." Rasch says such technology would go a long way toward eradicating such online nuisances as porn spam and spyware. "We will never fully automate the reading of contracts or agreements online. Nor would we want to -- after all, Internet lawyers need jobs, too. But by automating the vetting of clickwraps or implied agreements we could make everybody sleep a little easier."

Category 38.6	US legislation & regulation concerning privacy
---------------	--

#### 2004-10-05 spyware legislation US House Representatives

NewsScan; http://www.washingtonpost.com/wp-dyn/articles/A9558-2004Oct5.html

HOUSE PUNISHES SPYWARE PERPETRATORS

The U.S. House of Representatives has voted 399-1 to pass the "Spy Act," which imposes heavy federal fines on those who secretly install "spyware" programs on people's computers to surreptitiously monitor their Internet activities. The bill was introduced by Rep. Mary Bono (R-Calif.).

# 38.7 Other legislation & regulation concerning privacy

Category 38.7 Other legislation & regulation concerning privacy

#### 2004-02-12 privacy Australian Federal Privacy Commissioner warning

NewsScan

AUSTRALIA WARNS ON PRIVACY

The Australian Federal Privacy Commissioner has warned companies about Web sites that don't adhere to security practices that protect the privacy of customers or visitors. The Commissioner said he was disappointed that businesses are still making fundamental errors and said there is no longer any excuse for not having privacy built into IT system re-design and or upgrades. (Office of the Federal Privacy Commissioner — News Release 12 Feb 2004)

Category 38.7 Other legislation & regulation concerning privacy

2004-11-09 New Zealand mobile phone voyeur crime photographs nudity prviacy legislation law

NewsScan; http://theage.com.au/articles/2004/11/09/1099781374972.html

KIWIS COMBAT MOBILE PHONE VOYEURS

A New Zealand law being debated will impose a three-year jail sentence on mobile phone voyeurs who take intimate photographs of people without their knowledge. The law will make it an offense to surreptitiously film intimate situations involving nudity or partial nudity where people would have a reasonable expectation of privacy. (The Age 9 Nov 2004)

## **38.8 Law enforcement & privacy**

Category 3	38.8	Law enforcement	&	privacy
------------	------	-----------------	---	---------

#### 2004-01-22 **ACLU states' crime database privacy threat**

NewsBits; http://www.usatoday.com/tech/news/2004-01-22-aclu-vs-matrix\_x.htm http://www.chron.com/cs/CDA/ssistory.mpl/business/2365475

ACLU: States' crime database a privacy threat

A seven-state crime database launched with \$12 million in federal funds is a more powerful threat to privacy than its organizers acknowledge, the American Civil Liberties Union alleged Wednesday after obtaining documents relating to the program. The law enforcement officials and private database company behind the Multistate Anti-Terrorism Information Exchange, or Matrix, contend it is merely an investigative tool that helps police quickly gather already- available information on suspects.

Category 38.8 Law enforcement & privacy

2004-02-11 VoIP wiretaps privacy federal US government Bush administration CALEA

DHS IAIP Daily;

http://news.com.com/2100-7352\_3-5157282.html?tag=nefd\_top

February 11, CNET News.com — Feds step up push to wiretap VoIP calls.

The Bush administration plans to ask the Federal Communications Commission to order Net telephony providers to comply with a law that would permit police to wiretap conversations carried over the Internet. In a series of letters made public Tuesday, February 11, the Justice Department said it is "currently drafting a request" that would invoke the 1994 Communications Assistance for Law Enforcement Act (CALEA). That law requires telecommunications carriers to rewire their networks to government specifications to provide police with guaranteed access for wiretaps. It is debatable whether CALEA's decade- old definition of "telecommunications carrier," crafted long before the Internet era, applies to Voice over Internet Protocol (VoIP) providers. If the FCC rules that CALEA's definitions are not a close enough fit for the fast- growing and somewhat amorphous VoIP sector, then the Bush administration could ask Congress to rewrite the law. Until earlier this month, the FBI had tried to block the FCC from considering VoIP's regulatory structure until the wiretap issue was resolved. But last week, the two agencies said they had reached an agreement allowing a vote on VoIP regulations to take place on Thursday.

Category 38.8 Law enforcement & privacy

privacy incident Australia sensitive documents files unauthorized access

2004-02-12 NewsScan

POLICE FACE SACK IN ONGOING PRIVACY INCIDENTS

Australian Police in Victoria are facing an embarrassing new privacy scandal after an internal audit found fresh evidence of improper access to confidential computer files. The audit has found up to 35 police have used the police Law Enforcement Assistance Program (LEAP) computer to check information on a security guard charged with manslaughter over the death of former Test cricketer David Hookes. All police who have accessed the files, other than homicide squad police investigating the death, are expected to be asked by ethical standards department police to justify their actions. Police who cannot give legitimate reasons face the sack. This incident comes in the wake of an investigation in 2003 into allegations that the files of 32 current and former Victorian Members of Parliament have been accessed without legitimate reason.

Category 38.8 Law enforcement & privacy

#### 2004-05-21 surveillance database integration crime terrorism homeland security

http://query.nytimes.com/gst/abstract.html?res=F60A17F63A5B0C728EDDAC08 94DC404482

New details about criminal information project known as Matrix, which combines state records culled by database company Seisint to give investigators fast access to information on crime and terrorism suspects, raise questions about its potential power; records show Matrix gave federal and Florida authorities names of 120,000 people who showed statistical likelihood of being terrorists, before program actually began, resulting in investigations and arrests; objections were raised because system includes information on innocent people as well as known criminals; officials involved with Matrix say statistical method was removed from final product due to privacy concerns (M)

## Category 38.8 Law enforcement & privacy 2004-08-04 Internet Net telephone tapping voice-over-IP VoIP law enforcement FBI DEA DoJ Federal Communications Commission FCC

DHS IAIP Daily;

http://www.reuters.com/newsArticle.jhtml?type=internetNews&s toryID=5873014

August 04, Reuters — FCC: Net phone calls must be able to be tapped.

Internet phone carriers such as Vonage should set up their systems so U.S. law enforcers can monitor suspicious calls, the Federal Communications Commission (FCC) tentatively ruled on 12 Wednesday, July 4. By a vote of 5-0, the FCC said "voice over Internet protocol," or VoIP, providers should be subject to the 1994 Communications Assistance for Law Enforcement Act, which ensures that law enforcers will be able to keep up with changing communications technologies. VoIP service is likely to replace much traditional phone service over the coming years, the commission said. The Justice Department, FBI and Drug Enforcement Administration have argued that they must be able to monitor suspicious calls no matter how they are made. Technology advocates have worried that the fast- growing service, which promises to slash costs by routing phone calls over the Internet, could be harmed by excessive regulation. The ruling does not affect other regulatory questions surrounding VoIP service, such as how it should be taxed, FCC Chairman Michael Powell said.

### **38.9** Surveillance

Category38.9Surveillance2004-01-05school Mississippi webcam monitor classroom chilling effect creativity

NewsScan

GO STAND IN THE CORNER AND WATCH THE WEBCAM

A public school in Mississippi is apparently the first to use webcam technology to make sure that students being punished for bad behavior don't miss out on what's happening in class. Cameras document everything that takes place in the classroom, good and bad alike. But Barry Steinhardt of the American Civil Liberties Union worries that the cameras could have a "chilling effect" on students and teachers by making them "feel under constant observation" and affecting "the willingness of teachers to be creative or to introduce unpopular topics." (USA Today 5 Jan 2004)

Category 38.9 Surveillance

#### 2004-01-05 US immigration tracking system foreigners surveillance

NewsScan

DIGITAL TRACKING SYSTEM FOR VISITORS

U.S. immigration authorities are now using a digital inventory control system called US-VISIT, designed to keep track of the movements of foreign visitors who enter the country with visas. US-VISIT (an acronym standing for United States Visitor and Immigrant Status Indicator Technology) requires that digital fingerprints and photos be taken of visitors as they arrive in the United States. Homeland Security undersecretary Asa Hutchinson says, "We are looking at two purposes: to increase security and to improve the integrity of immigration control. A key thing is that we will be able to know who is overstaying their visa and violating the terms of their admission to this country." (Los Angeles Times 5 Jan 2004)

Category 38.9 Surveillance

#### 2004-01-05 webcam monitoring surviellance school

NewsBits; http://www.usatoday.com/tech/webguide/internetlife/2004-01-05-class-webcams\_x.htm

Webcams keep suspended students on track

Fredreka Schouten, writing in USA TODAY, reported on a Mississippi high school where suspended students watch teachers through Web cameras and microphones. In addition to helping students who are being punished for bad behavior avoid even more damage to their scholastic progress, the system allows classes to be archived for several weeks -- helpful for students who are ill or who want to review. Privacy advocates are concerned about possible harm from the surveillance. "Distance learning is a legitimate use of cameras in the classroom 'as long as the purpose is learning and they are not there as a pretext for another use,' says Barry Steinhardt, director of the American Civil Liberties Union's technology and liberty program. But he says he worries that cameras also could have 'a chilling effect on the speech of students.'" Schouten adds, "They feel under constant observation,' Steinhardt says. 'And it affects the willingness of teachers to be creative or to introduce unpopular topics.'"

 Category 38.9
 Surveillance

 2004-04-27
 public surveillance privacy Florida town background check law enforcement databases

NewsScan

WANT ATTENTION? DRIVE THROUGH MANALAPAN, FLORIDA

Manalapan, Florida, where two out of every three homes are worth more than \$500,000, will soon be running background checks on every car and driver that passes through town. Cameras will take infrared photos recording a car's tag number, and computer software will automatically run the numbers through law enforcement databases; police will also have a picture of the driver, taken with another set of cameras. A Manalapan police official says, "Courts have ruled that in a public area, you have no expectation of privacy." In any event, the official makes a point of saying that the data collected this way will be destroyed every three months. (AP/USA Today 27 Apr 2004)

### Category38.9Surveillance2004-05-05handhelds federal government surveillance

DHS IAIP Daily;

http://www.fcw.com/geb/articles/2004/0503/web- derby- 05- 05- 04 .asp

May 05, Federal Computer Week — Officials take surveillance STEPs.

At this year's Kentucky Derby, local, state and federal law enforcement and emergency management officials were keeping an eye on Churchill Downs using handheld devices, wireless connectivity, and a geospatial application that tapped into surveillance cameras. In the joint operations center, officials could access information and view maps through a geospatial application called Spatial Templates for Emergency Preparedness, or STEPs. The software collects geographic information system (GIS) data from disparate databases and makes it accessible through a Web portal. With STEPs, officials could monitor weather from their computers, access digital map data previously available only in hardcopy form and use 3- D visualization software to see the infield and stage emergency response personnel or vehicles, Langley said. Agencies involved included local police, emergency officials and homeland security personnel; Kentucky state police and the National Guard; and agents from several federal agencies such as the FBI, the Bureau of Alcohol, Firearms, Tobacco and Explosives, the U.S. Marshals Service and the Secret Service. Users as far away as Washington, DC, could also access the portal.

Category 38.9 Surveillance

#### 2004-05-24 **ID tracking passport foreign visitors**

DHS IAIP Daily; http://news.com.com/2100-7348-5219101.html

May 24, New York Times — U.S. nearing deal on way to track foreign visitors.

The Department of Homeland Security is on the verge of awarding the biggest contract in its young history for an elaborate system that could cost as much as \$15 billion and employ a network of databases to track visitors to the United States long before they arrive. The program, known as US- Visit and rooted partly in a Pentagon concept developed after the terrorist attacks of 2001, seeks to supplant the nation's physical borders with what officials call virtual borders. Such borders employ networks of computer databases and biometric sensors for identification at sites abroad where people seek visas to the United States. With a virtual border in place, the actual border guard will become the last point of defense, rather than the first, because each visitor will have already been screened via a global web of databases. Visitors arriving at checkpoints, including those at the Mexican and Canadian borders, will face "real- time identification"- - instantaneous authentication to confirm that they are who they say they are. American officials will, at least in theory, be able to track them inside the United States and determine if they leave the country on time.

Category 38.9 Surveillance

#### 2004-06-23 wireless WiFi police handheld devices surveillance database anti-terrorism

NewsScan

WIRELESS COPS AT THE AIRPORT

State troopers patrolling Boston's Logan International Airport will be using Blackberry handheld wireless devices to search the database of a company called LocatePLUS, which holds billions of online public records. The database was developed by aggregating and integrating a number of

databases to create what the company's chief executive calls a "complete dossier" on an estimated 205 million people. State Police Lt. Thomas Coffey calls the system "invaluable" and says "it really provides us with information that we probably could not obtain elsewhere without a lot of legwork." LocatePLUS has more than 15,000 customers, including more than 2,000 law enforcement agencies. (AP/USA Today 23 Jun 2004)

Category 38.9	Surveillance
2004-09-09	Chicago surveillance network cameras emergency suspicious behavior

NewsScan

CHICAGO PLANS NEW SURVEILLANCE NETWORK

Chicago mayor Richard Daley says his city's going to install a network of more than 2,000 surveillance cameras to alert authorities to suspicious behavior or emergency situations. Daley says, "Cameras are the equivalent of hundreds of sets of eyes. They are the next best thing to having police officers stationed at every potential trouble spot." Software would be used to detect unusual activity, such as a bag being abandoned in a stairwell or movement in an off-limits area. Daley dismisses privacy concerns, on the grounds that cameras will be installed only in public places (where a police officer would have a perfect right to check what's going on). (AP/USA Today 9 Sep 2004)

## Category 38.9 Surveillance 2004-10-11 government chat rooms surveillance statistical profile research grant homeland security Combat Terrorism mathematical model

NewsScan; http://www.washingtonpost.com/wp-dyn/articles/A25272-2004Oct11.html

U.S. GOVERNMENT FUNDS CHAT ROOM SURVEILLANCE

The U.S. government is funding a year-long study by a Rensselaer Polytechnic Institute computer science professor aimed at developing mathematical models to identify patterns in the chaotic traffic generated by online public forums that might reveal "hidden communities" of terrorists. RPI professor Bulent Yener will download data from selected chat rooms while tracking the times that messages were sent in order to create a statistical profile of the traffic. For instance, if QTpie and RatBoi consistently send messages within seconds of each other in a crowded chat room, it might be inferred that they are "speaking" to each other, camouflaged by the "noise" of the chat room environment. "For us, the challenge is to be able to determine, without reading the messages, who is talking to whom," says Yener. The \$157,673 grant to conduct the study comes from the National Science Foundation's Approaches to Combat Terrorism program, which works in concert with U.S. intelligence agencies to make its selections. However, some scholars doubt the concept has much merit: "In a world in which you can embed your message in a pixel on a picture on a home page about tea cozies, I don't know whether if you're any better if you think chat would be any particular magnet," says Harvard Law School Internet scholar Jonathan Zittrain.

## **38.A Medical / HIPAA**

#### Category 38.A Medical / HIPAA

2004-01-04

#### eICU hospital monitoring remote medical monitoring treatment examination

NewsScan; http://www.latimes.com/technology/ats-ap\_technology12jan04

'ENHANCED INTENSIVE CARE': IF YOU NEED IT YOU'LL WANT IT

New technology known as eICU ("Enhanced Intensive Care") lets physicians miles away from their patents manage health care via cameras and banks of computer screens. Developed by Baltimore-based VISICU Inc., the technology is already in use at least 18 hospital systems nationwide. Whereas traditional health care systems rely on nurses to notice a problem with a patient and relay the information to a doctor, eICU informs the doctor directly. The doctor can check the patient's ventilator, intravenous medication and anything else in the patient's room, and one physician notes: "The camera is such that I can count eyelashes." (AP/Los Angeles Times 4 Jan 2004)

Category 38.A	Medical / HIPAA
2004-01-27	HIPAA medical information security privacy WebMD delay
NIPC/DHS	

AMA Complains WebMD Mishandling HIPAA Claims Jan. 27, 2004

Problems with WebMD's handling of claims leads to hundreds of thousands of dollars worth of delayed and denied payments, and caused some doctors to revert to paper.

The American Medical Association has sent a letter to WebMD Corp.,likely the medical industry's most powerful player in electronic insurance-claims processing, complaining that it has mishandled claims submitted by doctors resulting in "hundreds of thousands of dollars" in delayed and denied payments, InformationWeek has learned. WebMD acknowledges there have been problems, but attributes them to implementing a new process. According to the letter dated Jan. 8, sent to WebMD CEO Roger Holstein and signed by the AMA and seven other medical associations, the frequency of physicians' complaints about WebMD has risen since the Health Insurance Portability and Accountability Act standards went into effect Oct. 16.In addition to setting standards regarding the privacy of patient information, HIPPA is intended to simplify and encourage electronic claims processing. But WebMD's efforts at HIPAA compliance appear to be having the opposite effect, according to the letter, a copy of which was obtained by InformationWeek. WebMD attributes any problems to the early stages of a new process.

Category 38.A Medical / HIPAA

#### 2004-01-29 HIPAA medical information security privacy WebMD delay

NIPC/DHS

Doctors Dependent on WebMD Despite Alleged Problems Jan. 29, 2004

Because of complexities with claims-processing and new requirements under HIPAA, doctors rely on WebMD and other clearinghouses to handle the work. The maturing field of Web-services technologies has the potential to let physicians' offices file medical claims directly to insurance companies using inexpensive Internet connections, eliminating the need for claims-processing clearinghouses. Yet some are convinced physicians will continue to depend on clearinghouses such as WebMD Corp., the biggest in the industry, because of the complex nature of electronic-claims processing. Doctors' offices "could use Web services" such as XML documents and the Simple Object Access Protocol to directly upload claims to insurance companies, says David Wroten, assistant executive VP of the Arkansas Medical Society. "But when a doctor's office tries, it immediately runs into little problems with different browsers," says Wroten, as Netscape Navigator and Microsoft Explorer each present the form differently. Rather than immerse themselves in technical details, offices rely on a clearinghouse to resolve problems and format the claim correctly. The majority of urban doctors' offices were using a clearinghouse before HIPAA was implemented Oct. 16. and have been reluctant to change since the new regulations went into effect, he says. But complaints about WebMD's inaccurate processing or lost claims were voiced in a Jan. 8 letter from the American Medical Association to WebMD CEO Roger Holstein. The letter said "thousands or hundreds of thousands of dollars" in delayed payments to some offices have resulted from mishandled claims.

## Category 38.A Medical / HIPAA 2004-02-09 HIPAA medical information security privacy compliance regulation insurance cost cut

#### NIPC/DHS

New Claim Game Feb. 9, 2004

Insurance companies want doctors to bypass clearinghouses and submit claims directly. The move could cut costs and complexities from the system.

On March 1, Harvard Pilgrim Health Care Inc. will take a drastic step to realize the savings intended by the federally mandated Health Insurance Portability and Accountability Act, which went into effect four months ago. The insurance company will no longer pay "click charges" of about 35 cents per transaction to WebMD Corp., the industry's largest medical-claims-processing clearinghouse, which handles a third of the 10 million claims Harvard Pilgrim pays out every year.

In addition to establishing rules to ensure patient privacy, HIPAA set standards for the electronic exchange of information that in theory should ease connection problems between health-care providers and insurance companies, while reducing costs associated with manually processing paperwork.

Do clearinghouses provide a valuable service or merely add unnecessary costs? The industry has long depended on them to aggregate claims coming from physicians' offices and send them in batches to the correct payers, at a cost of about \$414 million a year to insurance companies, according to Forrester Research. As the largest claims processor, WebMD is stumbling in its efforts to convince the industry that its clearinghouse adds value.

HIPAA undoubtedly is creating complexities in health care. For one, it specifies different formats for different functions, such as eligibility inquiries versus remittance responses. Claims also must be compliant in their content, which creates problems when a physician uses an old or rudimentary practice-management system for patient records and billing information. Fixing that can require intensive technical work between the physician's office and the clearinghouse and between the clearinghouse and the claim payer. But companies like Harvard Pilgrim don't see any savings being realized if WebMD becomes that dictator. Clearinghouses only add costs, Grose says. "It's a philosophical issue. WebMD just happens to be the one we disagree with most."

Category38.AMedical / HIPAA2004-02-20privacy medical records e-mail STDs partners notified

NewsScan

YOU'VE GOT...

Public health officials in Los Angeles County in California are using e-mail to notify the partners of people who had been diagnosed with STDs. The director of programs at the AIDS Project Los Angeles says: "My reaction is, bravo. I think this is really appropriate, given the role the Internet seems to play in the transmission of the diseases. I think this is a good use of technology that the target population uses and understands. This program was just initiated in San Francisco a couple of months ago. It's real innovative." (Los Angeles Daily News 20 Feb 2004)

Category 38.A Medical / HIPAA

2004-12-07 medical records Massachusetts eHealth pilot project doctors patients

NewsScan; http://www.latimes.com/technology/ats-ap\_technology14dec07

MEDICAL RECORDS-SHARING IN MASSACHUSETTS

If a new Massachusetts "eHealth" pilot project is successful, physicians in that state will be able to access patients' records from any hospital or clinic by computer. Gov. Mitt Romney says that switching from paper records to easily shared electronic records could save the state millions of dollars while improving patient safety and quality of care. He has given assurances that the system will have strict controls to allow patients to control who sees their records. (AP/Los Angeles times 7 Dec 2004)

#### Category 38.A Medical / HIPAA

2004-12-20 medical automated medication errors quality assurance bugs flaws training people human factors

NewsScan; http://www.washingtonpost.com/wp-dyn/articles/A15178-2004Dec20.html

AUTOMATED MEDICATION WORSE THAN THE DISEASE?

A report from U.S. Pharmacopeia (USP), a nonprofit group that sets standards for the drug industry, says that as more hospitals have implemented automated systems for administering drugs the number of errors associated with them has risen. USP vice president Diane Cousins says, "It would seem logical that applying computer technology to the medication use process would have a significant positive impact in preventing medication errors. Yet, depending on the computer's design or user competence, new points of potential errors can emerge." Kenneth Kizer of the National Quality Forum agrees with Cousins: "Technology offers great opportunity to reduce errors, but it's not a panacea. You can't just throw a computerized system in and expect that everything's fixed. It has to be done right. The technology is only as good as the people who use it." (Washington Post 20 Dec 2004)

# I&A products (tokens, biometrics, passwords, Kerberos)

Category 43 I&A products (tokens, biometrics, passwords, Kerberos)

#### 2004-06-01 password-plus identification authentication I&A two-factor theft

NewsScan; http://www.washingtonpost.com/wp-dyn/articles/A5693-

2004Jun1.html

**43** 

#### ARE PASSWORDS PASSÉ?

Scandinavian countries are at the forefront of a movement to ditch conventional asswords in favor of so-called two-factor authentication. These "password-plus" systems use things like disposable cards with scratch-off codes in conjunction with the usual four-digit PIN for online banking and other secure transactions. Each code is used once, and the bank replenishes the supply by sending a new card when the customer is running low. "A password is a construct of the past that has run out of steam," says Identix CEO Joseph Atick. "The human mind-set is not used to dealing with so many different passwords and so many different PINs." Other "password-plus" options include Vasco Data Security International's pocket-sized device that issues a random second code each time you type your regular password in. Or MasterCard International's system, which requires swiping your "smart" credit card through a special reader and entering your PIN to obtain a single-use password good at Office Max, British Airways and a dozen other merchants. And while U.S. banks are well aware of the perils of password theft, they're "all afraid of making the first step," says a Gartner analyst. "They don't want consumers going to other banks because it's too hard." (AP/Washington Post 1 Jun 2004)

## 43.2 Biometrics

Category 43.2	Biometrics
2004-02-17	biometric authentication passports air travel Europe

NewsScan

FINNISH GROUP GETS FIRST ORDER FOR BIOMETRIC PASSPORTS

Finland's Setec has received its first order for 3 million passports containing the new biometric technology required by the International Civil Aviation Organization and the U.S. government. U.S. law requires 27 countries, mostly in Europe, to issue biometric passports after Oct. 26, 2004, or require their citizens to apply for visas to visit the U.S. Setec's first order comes from Denmark, which is implementing the new passports this year, although current passport holders won't be required to upgrade until their current documents expire. (AP 17 Feb 2004)

Category 43.2 Biometrics

#### 2004-04-27 fingerprinting Ohio schools PIN biometrics meal plan

NewsScan

FINGERPRINT TECHNOLOGY IN OHIO SCHOOLS

The Akron, Ohio school district has begun using a \$700,000 "iMeal" program that identifies students in school lunch lines using their fingerprints. Students whose parents don't want them fingerprinted can instead be issued a PIN number to participate in the school lunch program. The coordinator of Akron's Child Nutrition Services says, "It's a parental and student choice what to do. We don't encourage or discourage either option." Whether students use fingerprints or PIN numbers, they'll be able to pay as they go through the lunch line or draw from a prepaid account. (AP/San Jose Mercury 27 Apr 2004) News

Category 43.2 Biometrics

2004-05-19 **biometric transportation aviation** 

DHS IAIP Daily; http://www.gao.gov/cgi- bin/getrpt?GAO- 04- 785T

May 19, General Accounting Office — GAO- 04- 785T: Aviation Security: Challenges in Using Biometric Technologies (Testimony).

The term biometrics covers a wide range of technologies that can be used to verify identity by measuring and analyzing human characteristics—relying on attributes of the individual instead of things the individual may have or know. Since the September 11, 2001, terrorist attacks, laws have been passed that require a more extensive use of biometric technologies in the federal government. In 2002, the General Accounting Office (GAO) conducted a technology assessment on the use of biometrics for border security. GAO was asked to testify about the issues that it raised in the report, the current state of the technology, and the application of biometrics to aviation security. The GAO found that three key considerations need to be addressed before a decision is made to design, develop, and implement biometrics into a security system: 1. Decisions must be made on how the technology will be used. 2. A detailed cost- benefit analysis must be conducted to determine that the benefits gained from a system outweigh the costs. 3. A trade- off analysis must be conducted between the increased security, which the use of biometrics would provide, and the effect on areas such as privacy and convenience. Highlights: http://www.gao.gov/nighlights/d04785thigh.pdf Source: http://www.gao.gov/cgi- bin/getrpt?GAO- 04- 785T

Category 43.2 Biometrics

#### 2004-05-20 biometric authentication credit card smart card

http://www.beepcard.com/products.asp; http://query.nytimes.com/gst/abstract.html?res=F60C17F8385B0C738EDDAC08 94DC404482

HI THERE! I'M YOUR OWNER!

Beepcard, a Santa Monica CA company, has introduced a smart card that could be used as a credit card with voice identification built-in. The authorized user would have to speak a registered password to activate the card.

[MK notes: Some known problems with voice pattern biometrics could be annoying. For example, depending on the sophistication of the algorithms, card might not recognize the authorized user if he or she were to have a cold.]

#### Category 43.2 Biometrics 2004-09-01 biometric identification authentication I&A fingerprint ID checkout supermarket Blockbuster Kroger PigglyWiggly ten-digit code

NewsScan

RETAILERS TEST BIOMETRIC CHECKOUT

Retailers, including Blockbuster, Kroger and PigglyWiggly supermarkets, are testing a finger-identification system that enables customers to pay for their goods just by placing their finger on a scanner and typing in a seven- to 10-digit code. "It's doing surprisingly well," says a PigglyWiggly spokeswoman. "The [customers] were a bit hesitant at first, but more and more of them have been able to grasp the concept each week." The supermarket chain plans to make the technology available in all 120 stores in the next few years. As finger-identification technology becomes increasingly common, companies are hastening to assure customers that they don't plan to share the information with others. Also, they point out that the system differs from government fingerprinting systems because finger ID records only unique data points -- instead of an entire print. (Wall Street Journal 1 Sep 2004)

#### Category 43.2 Biometrics

### 2004-09-09 Microsoft password solution list Windows XP Fingerprint Reader biometric authentication I&A

NewsScan

MICROSOFT POINTS TO PASSWORD SOLUTION

Microsoft has a solution for those who have difficulty keeping track of all the passwords and usernames required by many Web sites today. Its Fingerprint Reader hooks up to PCs running the XP operating system and scans the unique skin patterns of the user's finger. The software then stores the image and uses it as a reference to restrict access to secure Web sites. Microsoft warns that the Fingerprint Reader is not intended to protect sensitive data, such as financial information, but informal testing showed it did a pretty good job of keeping non-authorized users out, and also withstood attempts to fool it using Silly Putty and Scotch tape. However, the company emphasizes that its Fingerprint Reader is all about convenience, rather than security. The device will hit the stores in mid-November, priced at \$54.95, and Microsoft is also incorporating the Fingerprint Reader in a new keyboard and wireless mouse. (AP 9 Sep 2004)

## Category 43.2 Biometrics 2004-10-11 biometrics fingerprints retina handprint facial recognition comparison benefits cost future sales passwords users

NewsScan; http://online.wsj.com/article/0,,SB109744462285841431,00.html (sub req'd)

#### LET YOUR FINGERS DO THE TALKING

Fingerprint technology appears to be the biometric identification method of choice, surpassing competing systems such as retina scanning, handprint geometry and facial recognition. "Fingerprints will be dominant for the foreseeable future," says Don McKeon, product manager for biometric security at IBM. One reason for its popularity is falling prices for fingerprint readers: Microsoft recently introduced a stand-alone model for \$54 and earlier this year American Power Conversion rolled out a model for PCs priced at \$45. Meanwhile, IBM said last week it would begin selling laptops with built-in fingerprint readers and Microsoft is marketing a fingerprint reader-keyboard and -mouse. International Biometric Group predicts sales of fingerprint readers will rise 86% to \$368 million this year, up from \$198 million last year, spurred by user rebellion against the myriad passwords computer users must now memorize. "Our parents didn't deal with the problem of remembering 20 passwords, and our grandkids won't even know what they are," predicts McKeon.

## 43.3 Passwords

Category	43.3	Passwords		
2004-02-1	12	SSN Social Security number unencrypted user ID e-	mail	
RISKS			23	19
USERID+	-PW = NONO	C		
	noted in RISK inencrypted, of	S that his corporate Web site sent him his userID (his SSN) and f course).	his password in the sam	e e-mail
DON'T D	O THAT.			

2004-04-19	password management policy awareness survey study
Category 43.3	Passwords

http://www.securitypipeline.com/news/18902074

Mitch Wagner of securitypipeline.com wrote a summary of an informal man-in-the-street survey in London concerning attitudes and behavior with respect to passwords. Sample size was small: 172 people replied to the questions. Results were not good.

Quoting from Wagner's report:

>• 53 percent of users said they would not give their password to a telephone caller claiming to be calling from their IT department.

• Four out of 10 knew their colleagues' passwords.

• 55 percent said they'd give their password to their boss.

• Two thirds of workers use the same password for work and for personal access such as online banking and web site access.

• Workers used an average of four passwords, although one systems administrator used 40 passwords, which he stored using a program he wrote himself to keep them secure.

• 51 percent of passwords were changed on a monthly basis, 3 percent changed passwords weekly, 2 percent daily, 10 percent quarterly, 13 percent rarely and 20 percent never.

• Many workers who regularly had to change their passwords kept them on piece of paper in their drawers, or stored on Word documents.<

Other findings:

 $^* \sim ^{3}$ 4 of the respondents said they would reveal their password in return for a chocolate bar [MK asks: but how would you know if they were telling the truth? They could get a chocolate bar in return for any old word.]

\* Many respondents explained in that there passwords were based on partners, children, football teams, and pets.

\* The most common password was "admin."

\* Most people said they would steal confidential information when changing jobs.

\* Most of the respondents admitted that they would not protect the confidentiality of salary information if the data were accidentally revealed to them.

### Category43.3Passwords2004-08-11password authentication weak I&A easy-to-guess

NewsScan

MOST PASSWORDS ARE EASY TO GUESS

Most Internet users choose easy-to-guess passwords such as their pet's name, according to a survey by Visa Europe. More than three-fourths of those polled said they choose passwords relating to friends, family and memorable dates. The favorites are nicknames (21%), birthdays and anniversaries (15%), pet names (15%), family members' names (14%) and memorable dates such as the Battle of Hastings and England's World Cup victory (7%). Two percent even reported using "password" as their password. "It is not surprising that loved ones and pet names top the most popular list as often people struggle to remember random characters or designated log-in codes and opt to choose their own. Of course, it is important that our passwords are personal and meaningful to us, but also that they are difficult to decipher and not easily guessed," says Visa Europe VP Hugo Bottelier. When choosing a password, Visa suggests avoiding words that appear in the dictionary, as well as words relating to personal information that could be inferred or guessed. The most preferable type of password would have random letters, numbers and punctuation. And for heaven's sake, don't write it down and leave it by your credit card or PC! (Silicon.com 11 Aug 2004)

#### Category 43.3 Passwords

#### 2004-08-11 easy to use passwords Internet users

DHS IAIP Daily; http://www.silicon.com/0,39024729,39123066,00.htm

August 11, silicon.com — Internet users still choosing easy to guess passwords.

Despite increased awareness about the need for secure passwords, internet users are still leaving themselves vulnerable to hackers by choosing easy to guess subjects such as their cat or partner's name. Over three- quarters choose passwords relating to friends, family and memorable dates, according to research into 1,000 internet users by Visa Europe. The favourites are nicknames, birthdays and anniversaries, pet names, family members' names, and memorable dates. All of those are details that basic social engineering techniques would uncover relatively quickly. To make matters worse a third of respondents said they use the same password for all their log- ins, while a quarter using it nearly all or most of the time. But the message about choosing hard to guess passwords does seem to be getting through to some people with 22 per cent opting for random letters.

Category 43.3 Passwords

### 2004-08-18 password authentication graphical user picture drawing USENIX security Draw-A-Secret scheme

DHS IAIP Daily; http://searchsecurity.techtarget.com/originalContent/0,28914 2,sid14\_gci1000783,00.html

August 18, SearchSecurity.com — Graphical passwords still far from picture perfect.

Given the explosion of data now held in devices, and the fact many employees still use easily guessed words to access them, more companies are eyeing graphical password schemes. New research suggests a major weakness in current graphics- based password programs, whether self- drawn or computer- generated, remains people picking obvious choices. This raises the success of brute- force attacks launched by illegal dictionary tools. In a study of the password scheme Draw- A- Secret, in which users make a picture in a grid that's then replicated for access, users typically draw symmetrical, identifiable objects in the middle of the grid. 9 According to research by Julie Thorpe, a Canadian scholar who presented during last week's Usenix Security Symposium in San Diego, CA, and her partner Paul van Oorschot, it takes only six days for a computer to run through all of the most common choices. Add 999 more machines and the time narrows to 8.7 minutes. One way to up the odds would be for organizations using this program to require a minimum number of strokes (five or greater) and more unique drawings, such as disjointed or off- centered objects, Thorpe said.

## 43.4 Kerberos

Category 43.4 Kerberos

2004-09-01 Kerberos authentication protocol open source vulnerabilities code execution attack

DHS IAIP Daily; http://secunia.com/advisories/12408/

September 01, Secunia — Kerberos V5 multiple vulnerabilities.

Multiple vulnerabilities have been reported in Kerberos V5, where the most serious can potentially be exploited by malicious people to gain access to protected corporate networks and execute arbitrary code. Patches are available (see patch matrix in the original advisories). Update to version 1.3.5, when it becomes available: http://web.mit.edu/kerberos/dist/index.html Original Advisories: http://web.mit.edu/kerberos/www/advisories/MITKRB5- SA- 2004- 0 02- dblfree.txt and http://web.mit.edu/kerberos/www/advisories/MITKRB5- SA- 2004- 0 03- asn1.txt

#### 43.5 Single sign-on

Category 43.5 2004-03-01	Single sign-on identification authentication I&A ISP Internet service provider wireless acces piggybacking theft services IP address	55
RISKS	23 23	2

RISKS

E-MAIL ROBBERY, THE EASY WAY

Ralf Ertzinger analyzed the unfortunate decision by T-Online on user identification and authentication:

"T-Online is Germany's largest Internet provider, and while this in itself is not a risk, T-Online has always used a unique approach towards POP3 mail delivery. When being connected via T-Online, one does not have to provide a username or password to connect to the T-Online POP3 server in order to fetch mail, since the user is identified by his IP address.

Combine this with the growing number of (unsecured) WLAN access points and DSL routers and you get to read other people's mail just by driving along the streets. T-Online is aware of the problem, and provides information to secure WLAN access points on their web site, but changing the POP3 identification system (which was introduced long before anyone thought of broadband Internet, connection sharing and wireless LAN) seems to be almost impossible, having millions of customers."

## 43.6 E-mail authentication (e.g., SPF & SenderID)

#### Category 43.6 E-mail authentication (e.g., SPF & SenderID)

### 2004-10-26 AOL Microsoft sender ID e-mail SPF Sender Policy Framework spoofing antispam forgery authentication SMTP headers IP address

NewsScan;

AOL ACQUIESCES TO MICROSOFT SENDER ID AUTHENTICATION SCHEME

America Online reversed itself and now says it will adopt Microsoft's Sender ID e-mail authentication technology. Sender ID is a hybrid of earlier Microsoft technology and the technology that AOL initially championed, Sender Policy Framework (SPF). Sender ID works by checking records in the central domain-name system to check whether the sender's computer is authorized to use the domain name on the message, eliminating the annoying tactic of "spoofing," or forging, return e-mail addresses. AOL says it will begin testing Sender ID on inbound e-mail by year's end, while at the same time continuing to test other e-mail authentication technologies, including Domain Keys from Yahoo, plus to Cisco Systems technologies. (Wall Street Journal 26 Oct 2004)

 Category 43.6
 E-mail authentication (e.g., SPF & SenderID)

 2004-11-11
 address antispam AOL authentication EarthLink e-mail forgery Framework FTC headers ID IP Microsoft Policy Sender SMTP spam SPF spoofing Yahoo zombie

NewsScan; http://www.washingtonpost.com/wp-dyn/articles/A41460-2004Nov10.html

AUTHENTICATION WON'T END SPAM, SAY EXPERTS

Panelists at a forum sponsored by the Federal Trade Commission warned that criminals are already one step ahead of major email authentication initiatives planned by major ISPs, including AOL, Microsoft, Yahoo and EarthLink. The ISPs are still testing and backing several different plans, but the basic idea is that the e-mail system would check that the block of Internet addresses assigned to an e-mail provider includes the specific numeric address of a message sender. If the numeric address of the sender doesn't correspond with addresses assigned to the purported mail service, a red flag would be raised. The problem with that scheme, said the panelists, is that a majority of spam is now launched by "zombie" machines controlled by remote spammers. E-mail from a zombie PC looks as if it is coming from a legitimate source -- because it is. In the first half of this year, it's estimated that an average of 30,000 computers a day were turned into zombies, according to Symantec. But despite these discouraging statistics, the experts still insisted that authentication is a vital first step, to be followed by a system that evaluates the "reputation" of senders, perhaps using a process that marks good e-mail with an electronic seal of approval. (Washington Post 11 Nov 2004)

## 44.1 Crypto algorithms

Category 44.1 Crypto algorithms

#### 2004-05-17 quantum cryptography European Union EU response Echelon

DHS IAIP Daily; http://www.computerworld.com/securitytopics/security/story/0,10801,93220,00.html

May 17, Computer World — EU seeks quantum cryptography response to Echelon.

The European Union (EU) plans to invest \$13 million during the next four years to develop a secure communication system based on quantum cryptography, using physical laws governing the universe on the smallest scale to create and distribute unbreakable encryption keys, project coordinators said on Monday, May 17. If successful, the project will produce the cryptographer's Holy Grail - - absolutely unbreakable code - - and thwart the eavesdropping efforts of espionage systems such as Echelon, which intercepts electronic messages on behalf of intelligence services. "The aim is to produce a communication system that cannot be intercepted by anyone, and that includes Echelon," said Sergio Cova, a professor from the electronics department of Milan Polytechnic and one of the project's coordinators. "We are talking about a system that requires significant technological innovations. We have to prove that it is workable, which is not the case at the moment." Major improvements in geographic range and speed of data transmission will be required before the system becomes a commercial reality, Cova said.

Category 44.1 Crypto algorithms

#### 2004-05-17 key exchange quantum cryptography NIST speed of light

DHS IAIP Daily; http://www.gcn.com/vol1\_no1/daily- updates/25948- 1.html

May 17, Government Computer News - NIST doing crypto key exchanges at the speed of light.

The National Institute of Standards and Technology (NIST) is pushing the speed limit on cryptographic key exchanges on its new quantum communications test bed. The May 3 issue of Optics Express, the online journal of the Optical Society of America, described a demonstration of NIST's quantum key distribution system that delivered usable bits in the form of individual photons at the rate of 1Mbps. The process involves sending individual photons—elemental particles of light—in different polarizations and orientations to represent individual bits. The laws of physics declare that observing an elemental particle such as a photon changes it, making eavesdropping essentially impossible. "Detecting a photon involves its destruction," said Charles Clark, chief of the Electron and Optical Physics division. "If someone tried to eavesdrop, they would induce an error rate that would be so high it would be noticed." The system does not encrypt data; it only exchanges bits that can be used for an encryption key.

Category 44.1 Crypto algorithms

### 2004-08-17 cryptographic algorithm weaknesses found MD5 SHA-1 US Digital Signature Standard DSS PGP SSL

DHS IAIP Daily;

http://news.com.com/Crypto+researchers+abuzz+over+flaws/2100 - 1002\_3- 5313655.html?tag=nefd.lede

August 17, CNET News.com — Crypto researchers abuzz over flaws.

News that mathematical functions embedded in common security applications have previously unknown weaknesses have recently surfaced in encryption circles. French computer scientist Antoine Joux announced Thursday, August 12, that he had uncovered a flaw in an algorithm called MD5, often used with digital signatures. Then four Chinese researchers released a paper that reported a way to circumvent MD5 and other algorithms. Eli Biham and Rafi Chen, researchers at the Technion institute in Israel, reported some early work toward identifying vulnerabilities in the SHA- 1 algorithm at the Crypto 2004 conference in Santa Barbara, CA on Tuesday, August 17. SHA- 1 is embedded in popular programs like PGP and SSL. It is certified by the National Institute of Standards and Technology and is the only signing algorithm approved for use in the U.S. government's Digital Signature Standard. The MD5 and SHA- 1 algorithms are known to computer scientists as hash functions. They take all kinds of input, from an e- mail message to an operating- system kernel, and generate what's supposed to be a unique fingerprint. If a malicious attacker could generate the same fingerprint with a different input stream, the cloned fingerprint - known as a hash collision - - would certify that software with a back door is safe to download and execute. It would help a crook who wanted to falsely sign an e- mail instructing that someone's bank account be emptied.

#### Category 44.1 Crypto algorithms 2004-10-15 quantum encryption authentication research Boston University BBN Bolt Beranek Newman photons

NewsScan; http://theage.com.au/articles/2004/10/14/1097607360143.html

NETWORK SECURITY SET FOR QUANTUM LEAP

It's a hacker's nightmare but a dream for bankers and spies: A computer network so secure that even the simplest attempts to eavesdrop will interrupt the flow of data and alert administrators to the snooping. The work by researchers at Harvard University, Boston University and BBN Technologies is the closest scientists have come to a realworld quantum encryption system that uses light particles called photons to lock and unlock information instead of random-number "keys."

## 44.2 Crypto products

Category 44.2 Crypto products

#### Internet browser security VPN VLAN SSL IPSec business

#### DHS/IAIP Update

2004-01-16

January 14, CNET News — Browser security takes off in VPNs.

Corporations are embracing a simpler, cheaper way of connecting remote workers to their networks - - Secure Sockets Layer (SSL) encryption. SSL is a significant step forward in Virtual Private Network (VPN) ease- of- use as an alternative to Internet Protocol security (IPSec). SSL technology has been embedded in most standard Web browsers for years. SSL VPNs enable access from virtually any Web browser, so they're a natural fit for remote access and extranet applications. For most Web- based applications, users don't have to use a client, making it easier to give access to the network. IPSec VPNs require the installation and configuration of software on all clients and can be clunky when it comes to remote access, often meaning interoperability issues that can leave many frustrated and stranded without access to critical network information. Most experts agree that the technologies are complementary. Though SSL VPN has many benefits, it also has its downside. One important element is end- point security. SSL VPN allows people to enter corporate networks via any Web browser, socompanies need to make sure that it has strong authentication to verify that users are authorized. It also needs strong policy management to ensure that people only access applications for which they have approval. As people can use any Web- enabled device for access, viruses from those machines can be transmitted to the corporate network.

Category 44.2 Crypto products

#### 2004-01-16 Internet browser security VPN VLAN SSL IPSec business

NIPC/DHS; http://news.com.com/2100-1033\_3-5140548.html

January 14, CNET News — Browser security takes off in VPNs.

Corporations are embracing a simpler, cheaper way of connecting remote workers to their networks — Secure Sockets Layer (SSL) encryption. SSL is a significant step forward in Virtual Private Network (VPN) ease-of-use as an alternative to Internet Protocol security (IPSec). SSL technology has been embedded in most standard Web browsers for years. SSL VPNs enable access from virtually any Web browser, so they're a natural fit for remote access and extranet applications. For most Web-based applications, users don't have to use a client, making it easier to give access to the network. IPSec VPNs require the installation and configuration of software on all clients and can be clunky when it comes to remote access, often meaning interoperability issues that can leave many frustrated and stranded without access to critical network information. Most experts agree that the technologies are complementary. Though SSL VPN has many benefits, it also has its downside. One important element is endpoint security. SSL VPN allows people to enter corporate networks via any Web browser, socompanies need to make sure that it has strong authentication to verify that users are authorized. It also needs strong policy management to ensure that people only access applications for which they have approval. As people can use any Web-enabled device for access, viruses from those machines can be transmitted to the corporate network.

Category 44.2 Crypto products

#### 2004-08-24 quantum encryption cryptology security improvement NIST optical test bed

DHS IAIP Daily; http://www.eet.com/article/showArticle.jhtml?articleId=30000 032

August 24, EE Times — Quantum encryption poised to tighten data security.

Quantum cryptology is starting to move out of the labs and into commercial systems that leverage advanced optical- networking technology. Three companies, Quantique SA of Geneva, Switzerland, MagiQ Technologies Inc. of Somerville, MA, and Tokyo- based NEC Ltd. have brought out encryption systems for optical networks that rely on fundamental physical laws to block eavesdropping. Also, a group based at Austria's University of Vienna is quickly moving toward a commercial quantum- encryption system. In a real- world experiment, a commercial bank and Vienna City Hall were connected via a fiber optic link that was run under the streets. The system was able to generate identical random sequences of bits at both ends of the fiber, and the key was used to send a secure bank transfer. However, some quantum- information experts, including experts at the National Institute of Standards and Technology (NIST), question whether quantum- encryption schemes are the absolute barrier to data theft claimed by proponents of the approach. NIST has a large effort in the area of data security and is attempting to stay ahead of the quantum- encryption game with a sophisticated optical testbed.

## 44.3 Steganography

Category 44.3 Steganography

### steganography data hiding software Steganos Germany law enforcement secret services

NewsScan

2004-06-30

STEGANOGRAPHY

The term "steganography" has come to mean the practice of hiding messages within graphics or music files. Fabian Hansmann of the German software maker Steganos explains: "Steganography has one big advantage -- that is you cannot prove that information exists. If you just use encryption, you will always see that there is a file that carries encrypted information." Hansmann characterizes his company's \$60 security software suite as a "paranoid option" for advanced users who have the time and interest to hide their data. But Steganos products are under constant scrutiny by law enforcement officials. Hansmann says, "We regularly have inquiries from government agencies of all kinds, from foreign secret services to local police departments in Germany." (Reuters/USA Today 30 Jun 2004)

## Category 44.3 Steganography 2004-08-15 cyberspace Internet café Al Qaeda refuge terrorism Homeland Security steganography

DHS IAIP Daily;

http://news.yahoo.com/news?tmpl=story&u=/latimests/20040815/ ts\_latimes/cyberspacegivesalqaedarefuge

August 15, Los Angeles Times — Cyberspace gives al Qaeda refuge.

Since Osama bin Laden and his followers were driven from their bases in Afghanistan, the al Qaeda terrorist network has demonstrated an increasing ability to exploit the Internet. Independent al Qaeda cells and the network's loose hierarchy use easily available encoding programs and simple techniques to exchange virtually undetectable messages between Internet cafes in Karachi and libraries in London. Messages can be embedded in image, sound or other files transferred over the Internet through a process called "steganography." The files cannot be distinguished without a decoding tool. The al Qaeda operatives are often people with everyday skills who have harnessed the Internet in a campaign against the United States and its allies. In an effort to gather information on potential recruits and donors, U.S. law enforcement agencies operate Websites that are set up to resemble extremist Islamic sites. Visitors leave an electronic trail when they enter the site. On the other side, al Qaeda can transmit false information to determine whether its members are being monitored by law enforcement.

# 45.1 PKI (Digital signatures / certificates)

Category 45.1 PKI (Digital signatures / certificates)

#### 2004-01-12 PKI digital signatures UK European ecommerce internet

NewsBits; http://www.securityfocus.com/infocus/1756

Digital Signatures And European Laws

Mirella Mazzeo published an extensive article reviewing legal aspects of digital signatures in the European context. She reviews the technology and recent administrative declarations of the European Community and concludes, "The PKI situation in Europe is still not consistent across all countries, however. Some countries, such as Italy, Austria, and Spain have well-developed infrastructure already in place; others such as Finland, Denmark, Germany, and France are still testing their PKI solutions. Further, some countries such as Holland and the United Kingdom have not even started deploying their public key infrastructure."

Category 45.1 PKI (Digital signatures / certificates)

2004-01-13 VeriSign certificate absence confusion insecure transaction connection

NIPC/DHS; http://verisign.com/support/vendors/exp-gsid-ssl.html

January 11, The Register — VeriSign dead cert causes net instability.

The expiration of one of VeriSign's master digital certificates on Wednesday, January 7, created confusion for Net users and glitches to the operation of some applications, notably Norton Anti-Virus (NAV). After the cert VeriSign used to sign other certs expired, the chain of trust was broken, leaving some aps unable to set up a secure connection. These apps then defaulted to trying to access Verisign's certificate revocation list server which, faced with a huge extra load, buckled under the pressure. Essentially, where there are problems, traffic needs to be directed to a new Global Server Intermediate Root CA. Users of Java aps and older IE browsers were affected by the issue but NAV users were worst affected. NAV Users saw their computers slow to a crawl and Microsoft office applications not starting properly because of the problem.Verisign has posted an advisory on the problem at the following Website detailing server updates needed to resolve application instability: http://verisign.com/support/vendors/exp-gsid-ssl.html.

Category 45.1 PKI (Digital signatures / certificates)

#### 2004-01-16 public key infrastructure PKI implementation government security

NIPC/DHS; http://www.gao.gov/highlights/d04157high.pdf

January 15, Government Accounting Office — GAO-04-157: Status of Federal Public Key Infrastructure Activities at Major Federal Departments and Agencies (Report).

The federal government is increasingly using online applications to provide access to information and services, and to conduct internal business operations. As such, strong security assurances are necessary to properly safeguard data. The Government Accounting Office (GAO) found that Public Key Infrastructure (PKI) and its associated hardware, software, policies, and people can provide greater security assurances than simpler means of authenticating identity, such as passwords. Twenty of the 24 agencies reported that they are undertaking a total of 89 PKI initiatives, now in various stages of development. Agencies continue to face challenges, however, in PKI implementation, many of which are similar to those faced in GAO's 2001 report on the issue. Policy and guidance is often lacking or ill-defined, including in technical standards and legal issues. Insufficient funding for the high cost of PKI technology also is a challenge. Interoperability continues to be an issue, as integrating PKI with other systems at times requires significant change or even replacement. Another challenge is the administrative burden of training personnel for use and management of PKI.

## 45.2 Digital cash

Category 45.2 Digital cash

#### electronic food stamps US Department of Agriculture debit cards advantages

2004-06-23 NewsScan

FOOD STAMP ERA OVER: THE SYSTEM GOES ELECTRONIC

Agriculture Secretary Ann M. Veneman has declared the end of the "paper era" of the food stamp program: "This month the food stamp program arrived in the 21st century. States are destroying the paper coupons, and we don't anticipate that we'll ever have to print them again." Everybody seems to like the new electronic debit cards -- the recipients avoid the stigma attached to the paper coupons, the grocers get paid faster, and the states find the electronic simpler and less open to fraud. Under the new system, each recipient has an account in which benefits are electronically deposited each month, and can be drawn on at the checkout line of a grocery store by

sliding a plastic card through the same device used for commercial debit or credit cards. One benefits recipient says that when he was a teenager he saw "addicts who would trade food stamps for drugs even though they had sick children starving," whereas with the debit cards "you have no choice but to purchase food." (New York Times 23 Jun 2004)

## Category 45.2 Digital cash 2004-08-02 banking Websites e-commerce Internet Explorer vulnerability flaw hole security threat

NewsScan

TOP BANKING SITES VULNERABLE: RESEARCHER

The Web sites of three of Australia's four big banks are susceptible to cross-site scripting attacks, according to a British tech professional who gained prominence last year when he discovered a URL spoofing flaw in Microsoft's Internet Explorer browser. Sam Greenhalgh, who recently tested the Web sites of several British financial services companies and found many of them susceptible to the same kind of attacks, said the flaw resulted from sites not "sanitizing" information the user submits before displaying the information on the page: "If the information contains HTML, those HTML tags will be included on the site. Among other things this allows an attacker to include a tag that instructs the page to load a JavaScript file from another Web site." Greenhalgh provided demonstrations of injecting HTML on the sites using scripts he wrote himself. (The Age 2 Aug 2004) Rec'd from John Lamp, Deakin U.

[Note: "cross-site scripting:" Causing a user's Web browser to execute a malicious script. One approach is to hide code in a "click here" hyperlink attached to a URL that points to a non-existent Web page. When the page is not found, the script is returned with the bogus URL, and the user's browser executes it. -- from the Computer Desktop Encyclopedia, v18.2. See < http://www.computerlanguage.com >]

## 45.3 Micropayments

Category 45.3 Micropayments

#### micrpayments sucessful big business iTunes BitPass

2004-09-07 NewsScan

MICROPAYMENTS MORPHING INTO A MEGABUSINESS

The news that micropayment firm BitPass has just raised \$11.75 million in venture capital and attracted former American Express Chairman James Robinson III to its board is signaling a resurgence in interest in micropayment systems that facilitate payment for digital content.

Jumpstarting the move -- following a series of crash-and-burn dot-coms like Flooz and DigiCash -- is the notable success of Apple's iTunes, which last week announced it had sold 125 million music downloads at 99 cents each. A recent study by TowerGroup indicates that the total market for Internet and wireless micropayments -- fueled by demand for digital content -- will increase by 23% annually over the next five years to \$11.5 billion by 2009. "What it comes down to is that there simply must be a viable transaction model for smaller-cost products to make a dollar off e-commerce sales, but I think with what we've seen already in digital media, it's clear that people are figuring out how to make it work," says a Jupiter Research analyst. (CNet News.com 7 Sep 2004)

### 45.4 E-payments / e-wallets / creditcards

Category 45.4 E-payments / e-wallets / credit-cards

#### 2004-10-15 credit card fraud software application program server limits rules alerts

NewsScan; http://theage.com.au/articles/2004/10/15/1097784019869.html

AUSTRALIAN FIRM IN PUSH TO CUT CARD FRAUD

A Queensland-based firm has begun a push to market a locally developed application, which it says can significantly reduce or eliminate credit card fraud. The Credit Card Scanning Protection System runs on the server of the financial institution. Each user is served a page where he or she can set personal parameters -- the type of credit card, level of alert and any additional data that needs to be input in order that a transaction can be completed. For example, apart from merely having a username and a password for gaining entry to one's account, a user can also set up his or her preferences so that a transaction does not go through unless the specified rules are met. Regular debits, and outlets to which regular payments are made can also be specified. And any time a transaction goes through, the customer can receive an alert, either by SMS or email, to a variety of devices.

Category 45.4 E-payments / e-wallets / credit-cards

2004-12-06 electronic payments checks

NewsScan; http://www.washingtonpost.com/wp-dyn/articles/A41858-2004Dec6.html

ELECTRONIC PAYMENTS HAVE OVERTAKEN CHECKS

In 2003, Americans made 44.5 billion payments via electronic transactions, compared to only 36.7 billion payments by paper checks. The trend toward electronic purchases has been accelerated by strong growth in the popularity of debit cards, which can now be used to buy almost anything. Jean Ann Fox of the Consumer Federation of America says, "They're quick and easy. You don't stand there and hold up everybody in line behind you. Plus, folks are moving toward electronic banking and paying bills electronically." But she warns: "It's getting very confusing for consumers, and companies have not upgraded their protections." (Washington Post 6 Dec 2004)

## 45.5 Watermarks / digital-rights management / copy protection

#### Category 45.5 Watermarks / digital-rights management / copy protection

### 2004-01-05 consortium technology companies anti piracy illegal file sharing intellectual property rights protection

NewsScan

#### NEW PLAN TO PROTECT AGAINST ILLEGAL FILE SHARING

A consortium of five major information technology companies is planning a new system to protect digital music, video and software from illegal file sharing., The members of the new consortium (dalled Project Hudson0 are Intel, Nokia, Samsung, Toshiba and Matshushita, and the consortium's approach will compete against various other copy protection systems being advanced by Microsoft, Sony and Royal Philips Electronics, Apple, RealNetworks, and others. Leonardo Chiariglione, who founded the group that developed the original MP3 digital audio compression standard, says: "Content should be as transparent as it is today with MP3. It should be movable anywhere and still be protected. If we stay with digital islands people have a legitimate excuse to piracy." (New York Times 5 Jan 2004)

Category 45.5 Watermarks / digital-rights management / copy protection

2004-01-06 copy protection Europe consumer group lawsuit

NewsScan

#### EUROPEAN CONSUMER GROUP SUES OVER LOCKED CDs

Test-Achats, a consumer rights group based in Belgium, says it's received some 200 complaints from music fans angry over copy-protected CDs whose technology prevents them from playing on some CD players. The group has filed suit against major record labels, asking EMI, Universal, Sony and BMG to stop releasing the locked CDs and to reimburse disgruntled buyers. Industry observers say the legal action is the biggest challenge yet to the music industry's efforts to thwart piracy through copy-protection technology. But a statement by the International Federation of the Phonographic Industry says the lawsuit was baseless: "European law is clear that record companies and other copyright holders have the right to protect their works through technical means." The lawsuit is expected to be heard in a Belgium court this week. (BBC News 6 Jan 2003)

Category 45.5 Watermarks / digital-rights management / copy protection

### 2004-03-03 filtering technology stop music file sharing peer-to-peer P2P intellectual property rights copyright

NewsScan

#### FILTERING TECHNOLOGY COULD PUT AN END TO ILLEGAL FILE-SWAPPING

Audible Magic has been making the rounds on Capitol Hill, touting the capabilities of its technology, which it says can block the swapping of copyrighted music. It works by identifying the "psycho-acoustical" properties of a piece of music — essentially the computer equivalent of listening to the song itself — which enables it to recognize all versions of a song, despite variations in recording qualities or other subtle differences. The company has attracted the attention of the Recording Industry Association of America, which is backing Audible's technology as one possible solution to illegal downloading. In past months, peer-to-peer executives have repeatedly told Congress that is technologically impossible or infeasible to install such filtering systems on their networks, but with the advent of Audible, some are backpedaling on those statements, saying that even if it works, mandating the use of such technology would be a mistake. Requiring filters "would amount to the anointment of a specific technology as the winner in what the (recording) industry has made a file-sharing war," says Adam Eisgrau, executive director of P2P United, a file-swapping trade association. Eisgrau says his group has asked for a demonstration of the Audible Magic technology, and RIAA chief executive Mitch Bainwol says he's happy to oblige: "The peer-to-peer community has said they are serious about filtering. But they've said they can't filter. We're saying, well, the good news is that you can." (CNet News.com 3 Mar 2004)

#### Category 45.5 Watermarks / digital-rights management / copy protection

#### 2004-03-08 P2P peer-to-peer filtering testing copyright infringement block

http://www.nytimes.com/2004/03/08/technology/08music.html?th=&pagewanted =print&position=

The RIAA publicized a new technology from AudibleMagic to identify copyrighted materials during transfer and block it. John Schwartz of the New York Times wrote, "Audible Magic executives say that their software can be used in devices that attach to computer networks, or it can be written into the file-sharing software from companies like Kazaa and Grokster. . . . File-sharing companies have argued that they cannot control copyright infringement on their networks. . . . Record industry executives, who have said that they are against government-ordered technology fixes for copyright problems, said that they are not asking Congress to act, at least at this time. Instead, Mr. Bainwol said, his industry would like to see the 'peer-to-peer' companies add the software to their wares." Two universities had already signed up to examine the new technology at the beginning of March 2004.

Category	45.5	Watermarks /	′ digital-rights n	nanagement /	copy protection	

#### 2004-05-08 peer-to-peer P2P file sharing music piracy flooding denial of service

http://www.wired.com/news/print/0,1294,63384,00.html

A computer science professor and graduate student at the University of Tulsa have been awarded a patent for a method of thwarting illegal file sharing on peer-to-peer networks by flooding the network with bogus files that look like pirated music. The software creates bogus files with attributes—such as file names and description tags—that make them look like the real thing, but they are in fact white noise, low-quality recordings or advertisements to buy the song. What's more, the software sends out thousands of decoys to frustrate P2P users with fruitless downloads.

## Category 45.5 Watermarks / digital-rights management / copy protection 2004-07-29 Apple Real hacker corporate information warfare copyright infringement digital rights management DRM violation

#### NewsScan

#### APPLE ACCUSES REALNETWORKS OF USING HACKER TACTICS

Apple has accused RealNetworks, a provider of digital-media services, of offering software that lets online music buyers play on a variety of devices songs intended for use only on Apple's iPod devices. Apple says that it's "stunned that RealNetworks has adopted the tactics and ethics of a

hacker to break into the iPod." The RealNetworks software in question is called Harmony, which Real describes as "the world's first digital-rights-management translation system that music buyers can use to transfer music from one secure music device to another. It supports devices made by Creative, iRiver, palmOne, RCA, Rio, Samsung, and others. Legal experts seem to think that unless Apple can prove that RealNetworks reverse-engineered Apple's iPod software, a case under the Digital Millennium Copyright Act (DMCA) would be very hard to win. But Mark Rasch, former head of the U.S. Department of Justice's computer crimes unit (and now senior VP of security services firm Solutionary Inc.) says: "The problem with the DMCA is that it gives more protection than copyright law and it allows companies to skew the market with a form of protectionism. It allows technological protectionism to be legally adopted, and it works to prevent people from coming to market with cheaper compatible products." (InformationWeek 29 Jul 2004) Rec'd fr. John Lamp

## Category 45.5 Watermarks / digital-rights management / copy protection 2004-08-16 digital rights management DRM meaning copyright ownership intellectual property rights bootleg online Internet

NewsScan

#### THE NEW MEANING OF OWNERSHIP IN THE DIGITAL AGE

When you buy a CD from a store, you "own" that music, and as long as you don't bootleg it or charge lots of people money to listen to it, it's yours. But if you purchase that same playlist online, in most cases you're purchasing the "rights" to the content which is "locked" by some type of

digital rights management software. Not only that, but those rights may change over time, dictated by the whims of the music company you get them from. For instance, Apple Computer recently upped the number of computers on which its iTunes music files can be concurrently installed from three to five, but there's nothing stopping it from making its DRM more restrictive in the future -- although the company says that's unlikely. Meanwhile, customers of RealNetwork's Rhapsody music service "rent" their songs for a monthly fee but can play them only on their PCs, not their MP3 players. All these variables mean that consumers will need to be better informed in the

future about what it is they're actually getting for their money, says Alan Davidson, associate director of the Center for Democracy and Technology: "DRM underscores the point that consumers are going to have to become a lot more sophisticated about what they're buying." (Wall Street Journal 16 Aug 2004)

Category 45.5 Watermarks / digital-rights management / copy protection

2004-08-24 digital rights management DRM Microsoft Time Warner EU

NewsScan

MICROSOFT/TIME WARNER DRM PLANS QUESTIONED IN EUROPE

The European Commission is examining a proposed agreement by Microsoft and Time Warner to acquire joint control of the U.S. firm ContentGuard, a company that develops digital rights management (DRM) technology. The purpose of DRM software is to protect digital files (including movies and music files) from illegal copying and use. (Reuters/USA Today 24 Aug 2004)

#### Category 45.5 Watermarks / digital-rights management / copy protection

#### 2004-12-03 watermarks movies iTrace piracy video compression authentication

NewsScan; http://www.usatoday.com/tech/news/techinnovations/2004-12-03-piracy-watermarks\_x.htm

#### WATERMARK TECHNOLOGY SEEKS TO STAMP OUT FILM THIEVERY

Scientists at Sarnoff Labs have developed a "watermarking" technology called iTrace aimed at reducing video piracy perpetrated by moviegoers who secretly tape new films with handheld video cameras in the movie theater. Sarnoff's Jeffrey Lubin used his background in perceptual psychology to devise a watermark that not only would be invisible to the movie viewer, but would also survive several generations of crude copying. "The Holy Grail example is someone takes a camcorder into a movie theater and pirates a movie, and then compresses it on a digital file and puts it on the Internet," says Lubin. The iTrace watermark emerges gradually, over a 5-second interval, to exploit the tendency of human vision to compensate and ignore images that change slowly, he says. The watermark is actually a sequence of shifting blobs that get either lighter or darker and endure throughout the film. Each copy has its own unique watermark that enables studios to track the origin of a pirated copy. "The applications for watermarking are not just for the final result, but it also gives us freedom to move images around during production so that if they get into the wrong hands, they can be traced back to the last rightful owner," says Larry Birstock, executive VP of postproduction firm Post Logic Studios. (AP/USA Today 3 Dec 2004)

## 45.6 Smart cards and other ecommerce security measures

Category 45.6 Smart cards and other e-commerce security measures

#### 2004-05-03 smartcard smart card ID Transportation Security Authority TSA Florida

DHS IAIP Daily;

http://www.thetrucker.com/stories/05\_04/0503\_smart\_card.html

May 03, The Trucker — Prototype 'smart card' ID developed in Florida.

The Transportation Security Administration (TSA), the Florida Trucking Association and Florida state agencies are cooperating on a prototype "smart card" ID to be used at all 14 of the Sunshine State's deep- water ports and eventually by truckers and other transportation workers across the country. In 48 to 72 hours from the time a trucker applied, he or she would get the card containing his or her embedded fingerprints and a chip that could be activated for each port, according to Sandra Lambert, director of the division of driver's licenses for the Florida Department of Highway Safety and Motor Vehicles. The card would be issued after a background check that would include sending pertinent information such as Social Security number, date of birth, and criminal background if any to the FBI in Washington, who would then return the data to local officials who would create and ultimately activate the card unless the driver had committed certain felonies, which would prohibit use of an access card.

0004.05 10	
Category 45.6	Smart cards and other e-commerce security measures

#### 2004-05-16 virtual account numbers credit card protection one-time hash temporary account ecommerce

http://www.nytimes.com/2004/05/16/business/yourmoney/16cred.html?th

Users of credit cards from Citibank, MBNA America (which sponsors some 5,000 different affinity cards) and Discover can ask for temporary credit-card numbers that are linked to their real account but expire after a single use. Users can either download software to generate these one-time cryptographic hashes of their account number or they can visit their supplier's Web site to obtain one on demand. In addition to preventing fraudulent misuse of their credit-card number, these temporary card numbers can also stop retailers from unauthorized renewals of subscription services.

#### SINGLE-USE CREDIT CARDS

To combat identity theft, credit-card issuers sometimes issue virtual account numbers, which you typically obtain by signing up at the company's Web site and then download software to your computer to get a new disposable account number before each purchase you make. The number can only be used at one merchant, whether for a single purchase or for a service with a recurring monthly charge. MNBA executive Jim Donahue says, "It certainly has yet to capture the majority of cardholders, but those who use it are very loyal to it." However, since account holders normally don't have to pay for fraudulent purchases made to their accounts, many of them see no personal advantage to going through the extra step of obtaining a virtual account number. (AP/USA Today 10 May 2004) [NewsScan]

Category 45.6 Smart cards and other e-commerce security measures

#### 2004-10-01 smart cards Matsushita memory RAM e-cash identification authentication I&A

NewsScan; http://www.siliconvalley.com/mld/siliconvalley/9809932.htm

MATSUSHITA'S SMART CARDS

Japanese electronics company Matsushita Electric Industrial is adding smart-card capabilities to its memory cards, in which an integrated-circuit (IC) chip inside the card connects wirelessly with a special reader-machine to enable cashless payments, open locks, and read personal IDs. In a demo of the card's capabilities, Matsushita showed how a soccer-game ticket could be downloaded to a memory card on a personal computer, transferred to a cell phone, and then used at the stadium gate to get in instantly.

Category 45.6 Smart cards and other e-commerce security measures

2004-10-07 smart cards Matsushita memory RAM e-cash identification authentication I&A

NewsScan; http://apnews.excite.com/article/20041007/D85IJ5C80.html

ALL-IN-ONE MEMORY CARDS

Matsushita Electric Industrial Co., which makes Panasonic brands, is now developing memory cards that can be used for a variety of purposes -- from making cashless payments to opening locks. In Japan, people are already using smart cards to board commuter trains, and cell phone models enable users to buy drinks from vending machines, pay restaurant bills and play games at a Tokyo arcade. Matsushita's smartSD Card features 128-megabytes of memory, compared with Sony's FeliCa smart cards, which have only 32 kilobytes of storage. The enhanced Matsushita model will enable users to download movies or music and provide secure storage for documents, says Matsushita director Masaki Akiyama.

## 45.7 Sales taxes on Internet commerce

Category 45.7 Sales	taxes on Internet commerce
---------------------	----------------------------

#### 2004-07-12 New Hampshire Internet chat room tax service providers unhappy

NewsScan

NEW HAMPSHIRE PLANS TO TAX INTERNET CHAT ROOMS, ETC.

New Hampshire's tax collecting agency is proposing a 7% tax on telephone and Internet services, including chat rooms, voice mail, Web mail and instant messaging. Carol Miller, president of the New Hampshire Internet Service Providers Association, says the rule would be a huge burden to providers and is "far beyond the scope of what the tax was meant for." Verizon spokesman Erle Pierce agrees with Miller: "This is like changing the way you collect a turnpike toll: Instead of taxing the vehicle, we're going to put a tax on all the passengers... You pay not only for the vehicle, but

for what you are carrying in it. I don't think that's what the legislative intent was." But New Hampshire's tax collectors insist the change is just an upgrade to technology that "has forged ahead at a dramatic pace." (AP/USA Today 12 Jul 2004)

## 45.9 E-shopping carts

#### Category 45.9 E-shopping carts

### 2004-11-09 e-commerce shopping carts flash usability utility ease-of-use user resistance frustration abandon give up quit

NewsScan; http://online.wsj.com/article/0

FLASH-BASED SHOPPING CARTS AIM TO CLOSE E-SALES

A recent study by DoubleClick shows that for every dollar spent on e-commerce sites, \$4.10 is left in abandoned shopping carts, and now a handful of e-shopping sites are taking steps to recapture some of those sales. The key is a streamlined checkout process that allows the shopper to perform more functions -- from changing the color of a clothing item to filling out credit card information -- without leaving the page. Proponents of the new systems say that by preventing shoppers from jumping from screen to screen in the final stages of a purchase, consumers are less likely to become frustrated and quit. And while the new checkout screens look just like a Web page, they're actually small software programs written using Macromedia's Flash software that dynamically update the bottom line -- including tax and shipping costs -- as the customer adds or deletes items. Billing and other information is verified as it is entered to prevent customers from moving forward in the process without valid data. The Flashbased carts are being used by TJX Companies, owner of the T.J. Maxx and HomeGoods chains, and by PC Connection, among others. "This technology is very much in keeping with our sense of wanting to make it convenient for customers to shop our stores," says TJX VP Sherry Lang. "Even in our stores, we have a bank of cash registers so customers are able to check out very easily." (Wall Street Journal 9 Nov 2004)

## 47 US computer-crime laws

Category 47 US computer-crime laws

#### 2004-05-24 identity theft insider theft punishments laws

DHS IAIP Daily; http://www.informationweek.com/story/showArticle.jhtml?artic leID=20900519

May 24, InformationWeek — Feds want tougher penalties for insider identity theft.

A federal proposal to combat identity theft takes a particularly hard line on people who abuse insider access to information to commit the crime. The House Judiciary Committee earlier this month passed a bill, the Identity Theft Penalty Enhancement Act, that would establish a new crime of aggravated identity theft and increase applicable penalties. The bill also includes an amendment that directs the U.S. Sentencing Commission to revise its guidelines to include stronger punishment for those who abuse a position of trust to commit insider identity theft. According to "Predator Profiles," a forthcoming report from Michigan State University's (MSU) identity- theft research center, at least half of identity theft now results from the theft of personal information stored on business databases. Noting that her organization's research has since been corroborated by two other studies, MSU researcher Judith Collins says that at least 50%, and potentially as much as 70%, of identity thefts originate in the workplace by employees or people impersonating employees. "Our research also showed that the majority of those identities were stolen first and foremost from health- care- related institutions, and secondly from financial institutions," said Collins.

## **48.2** Non-US computer-crime laws

Category 48.2 Non-US computer-crime laws

2004-03-03 data theft prevention government guidelines Japan

NewsScan

JAPAN MOVES ON DATA THEFT

Concerned about high-profile incidents where customer data has been stolen, the Japanese government has stepped in. Japan's Ministry of Economy, Trade and Industry has drawn up a draft set of guidelines that will require Internet service providers to secure data by appointing security managers. (Daily Yomiuri 3 Mar 2004,rec'd from John Lamp, Deakin University)

Category 48.2 Non-US computer-crime laws

2004-04-13 anti-stalking laws Australia ISP concern Net-hard cyberstalking

NewsScan

AUSTRALIAN STALKER AMENDMENTS CONCERN ISPS

Tough amendments proposed to Australian federal laws designed to slam the lid on pedophiles and Internet stalkers could leave ISPs carrying the can for "menacing, harassing or offensive" behavior by subscribers. The move -- part of Australia's Crimes Legislation Amendments (Telecommunications Offences and Other Measures) Bill -- adds the weight of criminal law to the Internet content regime, which uses a takedown system to remove offensive material. Internet lobby groups have warned the amendments could force ISPs to make decisions on removing content subject to complaints without an independent review. The amendments have not yet been introduced to Parliament. The proposal to hold ISPs liable for offensive content is a sticking point in the omnibus legislation, which also criminalizes mobile-phone cloning, making death threats online, transmitting child pornography and "grooming" or procuring children. Although the legislation indemnifies ISPs if they are not aware of offensive content, it requires them to remove content they have been made aware of. (The Australian 13 Apr 2004)

Category 48.2 Non-US computer-crime laws

#### 2004-06-08 anti-trust European Union lawsuit Microsoft appeal

NewsScan

MICROSOFT TO APPEAL EU ANTITRUST DECISION

Microsoft has filed an appeal of the European Union's antitrust decision requiring the company to change business practices deemed detrimental to competition. Microsoft says that to follow the EU's ruling would undermine global innovation: "We believe that the interest of consumers and other European companies should be at the heart of this case. The Commission's decision undermines the innovative efforts of successful companies" -- and would "significantly alter incentives for research and development that are important to global economic growth." EU Competition Commissioner Mario Monti says he's confident that the Microsoft appeal will fail. (AP/USA Today 8 Jun 2004)

Category 48.2 Non-US computer-crime laws

#### 2004-07-02 Microsoft anti trust laws violation China Bill Gates compliance

NewsScan

GATES UNFAZED BY POSSIBLE CHINESE ANTI-TRUST LAWS

Microsoft chief Bill Gates says he's not concerned about the possibility of China introducing anti-trust laws even as his company faces further accusations of anti-competitive behavior. "We already do business in over 50 countries that have laws like that and we are in full compliance with those laws. I don't expect any problems, nor did it come up [during meetings with Premier Wen Jiabao]." Last month the official Xinhua news agency reported that the central government was considering a draft anti-monopoly law aimed at curbing anti-competitive behavior by multinational companies after a report found firms such as Microsoft have been allegedly "abusing their advantageous positions to curb competition." In March the European Union accused the software giant of abusing its "near

monopoly" with its Windows software. (The Age 2 Jul 2004) Rec'd from John Lamp

Category 48.2	Non-US computer-crime laws
2004-08-04	Vietnam Internet censorship police government intervention information access
NewsScan	
VIETNAM SETS U	P FORCE TO POLICE NET
official said: "Firstly Vietnam. We will also other criminal activit four million people of	Force will begin operations next month to fight cyber-crime in Vietnam. A Ministry of Public Security we will punish those who develop or intentionally transmit viruses to sabotage the computer network in to attempt to prevent les from being conducted over the Internet and will try to block pornographic Web sites." Only around ut of a population of 81 million people regularly surf the Internet in Vietnam, mainly through cyber-cafes. A) Rec'd from J Lamp
Category 48.2	Non-US computer-crime laws
2004-08-11	new tough cyber crime law Zambia non-US network vandals jail
NewsScan	

ZAMBIAN PARLIAMENT PASSES TOUGH CYBERCRIME LAW

A tough new law enacted unanimously by Zambia's parliament would see convicted network vandals and other cybercrime offenders get jail sentences ranging from 15 to 25 years. The government said the new law would help curb cyber crimes that had become a problem in the poor southern African country where only one in a thousand people have access to computers. (The Age 11 Aug 2004) Rec'd from J. Lamp

## 4A7 Spam

Category 4A7	Spam
2004-01-11	anti spam law ineffective guidelines junk e-mail

NewsScan

ANTI-SPAM LAW ENACTED - SO WHAT'S ALL THIS JUNK IN MY IN-BOX?

The new federal anti-spam law went into effect Jan. 1, but consumers report their inboxes are more cluttered than ever — what's going on? Critics say the new law doesn't actually ban spam but rather provides guidelines for sending junk e-mail legally. "Now we have a green light for what would come to be called 'legal spam,'" says ePrivacy Group CEO Vincent Schiavone. John Levine, a board member of the Coalition Against Unsolicited Commercial E-Mail, concurs: "Basically, it's a bill of rights for companies that want to send junk e-mail." In addition, the federal law supercedes stricter laws recently passed in several states, such as California. "Everyone was planning for this California law, which was so draconian," says a California lawyer who defends accused spammers. "Once the federal government passed the federal law, everyone was kind of relieved." And while technology firms are eagerly pursuing new ways of blocking spam, skeptics say the ultimate solution won't be technological or legal, but will depend on developing more savvy users. Mary Youngblood, abuse team manager at EarthLink, suggests putting numbers in the middle of your e-mail address to make it more difficult to guess and using a separate address for online shopping and newsgroup postings. (AP Jan 11 2004)

Category 4A7 Spam

#### 2004-01-20 anti spam CAN act ineffective

NewsScan

ANTI-SPAM LAW LARGELY IGNORED

The new federal anti-spam law ("Can Spam") doesn't seem to being changing the practices of the largest spammers: most of the largest bulk e-mailers are continuing to send illegal mass mailings for porn, get-rich-quick schemes and miracle drugs. The spam-filtering company Brightmail says that about 58% of e-mail monitored in January has been spam, in defiance of the new law, which took effect at the beginning of this month. The only real impact of the law seems to have been felt by small businesses, many of which have decided to discontinue e-mail marketing. One business, calculating that it would cost \$100,000 a year in personnel and technology to make its e-mail system comply with the law, decided to switch its advertising campaigns to Microsoft MSN and Yahoo. (USA Today 20 Jan 2004)

Category 4A7 Spam

#### 2004-01-29 FTC spam relay user responsible secure servers software

NewsScan

FTC WARNING PUTS ONUS ON COMPUTER USERS

The Federal Trade Commission and regulatory agencies in 26 countries have sent out letters to hundreds of thousands of computer users, warning them that spammers are lurking in cyberspace, waiting for the opportunity to hijack their servers and route junk e-mail through them. Spammers often use unsecured computers to disguise the origin of their messages. "Recipients may think the spam comes from your system," said the FTC's e-mail message. "Securing your server will help you protect your system from being misused." Don Blumenthal, coordinator for the FTC's Internet lab, admitted the agency did not attempt to verify that each computer targeted by the warnings was actually vulnerable to hacking, but said the message urged recipients to visit the FTC Web site for more information on properly configuring their software. (AP 29 Jan 2004)

Category 4A7	Spam
2004-02-03	antispam law legislation bill CAN-SPAM

NWF http://www.nwfusion.com/newsletters/sec/2004/0202sec1.html

Can CAN-SPAM Can Spam?

By M. E. Kabay, PhD, CISSP

On January 1, 2004, The CAN-SPAM Act of 2003 took effect in the United States. The Act is formally entitled, "Controlling the Assault of Non-Solicited Pornography and Marketing Act of 2003" and was introduced as S. 877 (passed Nov 25, 2003) and accepted by the House on Dec 8, 2003 [1].

Critics have consistently attacked the law as inadequate to control spam on the following grounds [2]:

1. The Act is based on an opt-out philosophy. Anyone can send one junk e-mail message legally as long as they offer an opt-out procedures. However, it is widely believed that many or most of the people who send spam value opt-out replies because they validate addresses. They then sell those addresses to other spammers. As a result, many people will be reluctant to use opt-out mechanisms. In any case, there are more than 20 million businesses in the USA today [3], so if every one of them chose to send a user exactly one message per year at random, a user could expect an average of over 54,000 messages requiring an opt-out response per day. If only 1% of these businesses chose to send out junk e-mail, the daily average would be 500 or more new junk messages requiring an opt-out.

Section 5(a)(3)(A) requires spammers to provide an opt-out mechanism, but describes these mechanisms broadly as including "a manner specified in the message, a reply electronic mail message or other form of Internet-based communication..."

As pointed out by blogger Ed Foster, this section means that a spammer could create an opt-out mechanism requiring an unwilling recipient to log on to a Web site and search for opt-out instructions, possibly while being bombarded by pop-up ads [4]. Can you imagine having to log on to Web site after Web site to unsubscribe from drivel you never asked for and detest on sight? Think of the time involved. Furthermore, Web-based opt-out instructions permitted under this law will make it difficult for automated systems to unsubscribe victims of spam using such mechanisms. [Note from MK: I remember one spammer who demanded that his victims \_solve a puzzle\_ in order to be freed from his waves of, ah, e-xcrement.]

2. Section 9 of the Act mandates a Do-Not-E-Mail Registry for no later than July 2004 but provides no details on how such a registry would be created and updated, how it would be protected against abuse by spammers, which government agency would control it or how it would be used to limit spam.

3. The Act defines "commercial electronic mail message" as "any electronic mail message the primary purpose of which is the commercial advertisement or promotion of a commercial product or service (including content on an Internet website operated for a commercial purpose)." This definition thus permits spam from politicians, political groups, religious organizations, charities, hate groups, hobbyists, cranks, and anyone else so long as the content cannot be construed as "commercial" (which is itself not defined in the Act).

4. CAN-SPAM overrides more restrictive state laws, weakening the range of legal countermeasures against spammers in the USA.

5. Nothing in the Act resolves the problem of spam directed against US residents but originating outside the boundaries of the USA.

By mid-January, anti-spam campaigners were confirming their pessimistic impression of the law's effectiveness. According to Jan Libbenga of \_The Register\_, "The NANAS sightings newsgroup (a large collection of spam, updated continuously) doesn't contain one spam message that is CAN SPAM compliant." [5]

Let's hope for some successful prosecutions of spamming soon with some stiff penalties. Until then, I'm sorry to say that I doubt that this law will have any helpful effect on spam.

\* \* \*

### Category4A7Spam2004-02-17spam laws strategy analysis

Network World Fusion

http://www.nwfusion.com/newsletters/sec/2004/0223sec1.html

Can Laws Block Spam?

by M. E. Kabay, PhD, CISSP Associate Professor, Computer Information Systems Norwich University, Northfield VT

I just read a new White Paper from Montreal-based Vircom, developer of Modus secure messaging solutions, on recent international anti-spam legislation efforts. Entitled, "Can Laws Block Spam?" the paper uses interviews with five experts on spam:

\* Lindsay Barton, Manager, Online Policy at the National Office for the Information Economy of Australia;

\* Anne P. Mitchell, Esq., President/CEO, Institute for SPAM and Internet Public Policy and Professor of Law, Lincoln Law School of San Jose, California;

\* Michael D. Osterman. President and Founder, Osterman Research

\* Troy Rollo, Chairman of the Coalition Against Unsolicited Bulk Email in Australia and Executive Director of the International Coalition Against Unsolicited Commercial Email

\* Neil Schwartzman, Editor & Publisher spamNEWS, Chair, Canadian Coalition Against Unsolicited Commercial Email

The paper analyzes the CAN-SPAM act in reasonable detail, but this column has already pointed readers to that legislation and analyses of its weaknesses. More interesting here is the analysis of the European Community Directive on Privacy and Electronic Communication Regulation 2003. This legislation provides for opt-in (not opt-out) restrictions on sending junk e-mail. Much as with fax messaging, no one may initiate e-mail marketing without prior permission or prior business relationship – and there must be an easy way to refuse future junk e-mail at the time of initial data collection about an individual. In addition to enforcement actions initiated by the Information Commissioner in law courts, victims of spam may also sue for damages of up to £5,000 in cases heard before a judge (unlimited if heard before a jury). However, critics point out that the law does not regulate business-to-business spam, including spam sent to employees via their business e-mail addresses.

Another section covers the Australian Spam Act of 2003, which includes not only e-mail spam but also SMS (Simple Message System) junk messages. This law also uses an opt-in strategy, in contrast with the US approaches that depend on opt-out methods. There are also clauses dealing with proper (accurate) origination addresses and restrictions on harvesting e-mail addresses automatically. Penalties are potentially much higher than in the US or in Europe: "Civil penalties under the Act will be assessed according to a sliding scale for repeat offenders. An individual could be liable for up to a total of A\$44,000 ... for contravention on a single day, while an organization could be fined up to \$220,000 AUD in a day. Offenders with a prior record will be penalized up to a maximum of A\$220,000 ... for each day of spamming by an individual, and A\$1.1million ... per day for organizations."

Although the Australian law has many admirable features, it founders on the reef of international spam. As commentators note in the White Paper, national laws will inevitably fail to control spam sent from outside their borders. According to a UNCTAD (United Nations Conference on Trade and Development) report on the origins of spam in 2003, the sources were 58.4% USA

5.6% China 5.2% UK 4.9% Brazil 4.1% Canada 21.8% Other

[On a side note, I have been receiving the most amazing junk e-mail from China lately – ads in comically bad English for everything from inflatable dolls the size of buildings to industrial flooring components and chemicals. Given that China has one quarter of the world's population and an economy that is growing at 9-11% per year, this trickle bodes very badly for the future of our inboxes.]

I think Michael Osterman summed up the situation well in his commentary: "Spam legislation, while well intended, will not control spam alone. The only answer is to fight spammers with the same weapon they use: technology. The problem with spam will be better faced by IT staff then by legislators. To control spam, it must be rendered economically non-viable. Now that is difficult to achieve because it costs virtually nothing to send; however, if we can increase the cost of sending a spam message, we can make it nonviable and the only way we can do that is through the increased use of anti-spam tools. . . . When anti-spam filters are effective they can eliminate 95% or more of the incoming spam, "...If an anti-spam filter can stop 95% of the spam that reaches an end user, the cost to the spammer of reaching that potential customer has risen by 20 times. Increasing the effectiveness of these filters to 97% increases the cost to the spammer by 33 times. The hope is that the potential revenue available to spammers drops by a corresponding amount, and equilibrium is reached."

Category 4A7 Spam

2004-02-18 spam AOL Earthlink Thailand route e-mail conspiracy theory

NewsScan

CONSPIRACY THEORY

Lawsuits filed yesterday by AOL and Earthlink accuse individuals and companies of running spam networks. The AOL suit alleges a conspiracy between three Floridians and two Americans living in Thailand to route mortgage-scam solicitations to AOL customers and to defeat AOL's spam filters through a company called Connor-Miller Software Inc. Earthlink is accusing 16 individuals and companies in Florida, California, Tennessee and Michigan of operating a multi-state spam operation that has sent more than a quarter of a billion e-mail messages promoting herbal supplements, Viagra and adult dating services and of using stolen identity documents to open Earthlink Internet accounts that were used to transmit the spam. The attorney who represents the Florida defendants in the AOL lawsuit argues that his clients are innocent of spamming: "They set up a network, just like AOL is a network." (Washington Post 18 Feb 2004)

Category 4A7 Spam

#### 2004-02-23 anti-spam act Australia April 2004

NewsScan

AUSTRALIAN SPAM ACT STARTS IN APRIL

The Australian Spam Act 2003 comes into force in April. The National Office for the Information Economy (NOIE) has produced helpful guidelines for business on how they should approach the sending of commercial electronic messages. The guidelines focus on compliance with the new legislation. (Spam Act 2003: Guides and Information Sheets Feb 2004)

Category 4A7 Spam

#### 2004-03-10 anti-spam lawsuit ISPs legislation Microsoft Earthlink Yahoo

NewsScan

ISPs SUE SPAMMERS UNDER CAN SPAM LEGISLATION

Teaming up in an unusual joint effort, Microsoft, MSN, EarthLink and Yahoo have filed six lawsuits against hundreds of people who allegedly have sent millions of spam e-mail messages through the plaintiffs' e-mail networks. The lawsuits mark the first legal action taken under the Can Spam legislation, which took effect on Jan. 1. "Congress gave us the necessary tools to pursue spammers with stiff penalties, and we in the industry didn't waste a moment moving with speed and resolve to take advantage of the new law," says AOL executive VP Randall Boe. Among the named defendants are Davis Wolfgang Hawke and Braden Bournival, both of whom are accused of sending millions of e-mails touting weight loss supplements, personal "lie detectors" and other products. Dozens of others are identified only as "John Doe" defendants. (AP/Wall Street Journal 10 Mar 2004)

Category 4A7 Spam

#### 2004-03-10 CAN-SPAM lawsuit spammers e-mail caller-ID address authentication spoofing

http://www.nwfusion.com/news/2004/0310microtoan.html

In March 2004, Microsoft, Yahoo and AOL announced lawsuits against spammers under the CAN-SPAM Act. In addition, they proposed technical measures to interfere with spoofing of e-mail addresses — what they termed Caller ID e-mail specification.

Category 4A7 Spam

#### 2004-04-29 CAN-SPAM law legislation prosecution

http://www.nwfusion.com/news/2004/0429canspam.html

In April 2004, two large spammers, Phoenix Avatar of Detroit MI and Global Web Promotions operating in Australia and New Zealand, were charged with violations of the CAN-SPAM Act. Phoenix Avatar officials were arrested for failing to include an opt-out address or a valid postal address in their junk and for using fraudulent FROM addresses. In addition, the accused mail fraud charges in federal court. The southern-hemisphere spammers were traced to buy cooperation with Australian and New Zealand authorities. All of the cases involved buying the bogus products and tracing money transfers to catch the crooks. Howard Beales, director of the FTC's Bureau of Consumer Protection, explained, "Rather than try to trace the e-mail, we tried to trace the money. It's virtually impossible to trace the spam itself."

## Category4A7Spam2004-05-01Australian spammer FTC pornographic marketing CAN-SPAM Act

#### NewsScan

U.S. TAPS AUSSIE SPAMMER

The U.S. government has launched its first criminal case against spammers, and taken civil action against an Australian spammer with the help of local authorities. The U.S. Federal Trade Commission says that the first charges have been brought against several U.S. companies under Controlling the Assault of Non-Solicited Pornography and Marketing (CAN-SPAM) Act, which took effect in January. It also has served legal notices on Australian company Global Web Promotions Pty Ltd, which investigators said pitched fraudulent weight-loss and growth-hormone products. The FTC says it brought its case with help by the Australian Competition and Consumer Commission and the New Zealand Commerce Commission. ACCC spokeswoman Lin Enright confirmed the ACCC assisted the FTC in tracking down Global Web Promotions, but would not say whether it would have a continuing role in the matter. (The Australian 30 Apr 2004, rec'd from John Lamp, Deakin University)

Category4A7Spam2004-05-19FTC explicit labels e-mail pornographic adult content subject line graphc bars

NewsScan

FTC DEMANDS "EXPLICIT" LABEL FOR "EXPLICIT" MATERIAL

A new Federal Trade Commission rule requires that unsolicited commercial e-mail containing adult-oriented material include a special label in the subject line; it also bars graphic images from appearing in the opening body of the message (to force a recipient to take at least some positive action to see the material he or she has been warned about in the subject line). FTC attorney Jonathan Kraden says the label should help the computers to filter if a computer user decides to set their filtering system up to recognize the label, but First Amendment lawyer Jonathan L. Katz warns: "This is a back-door effort to violate people's First Amendment rights, whether well-intentioned or not." Spammers who violate the rule face possible imprisonment and criminal fines of up to \$250,000 for individuals and \$500,000 for an organization. (AP/San Jose Mercury News 19 May 2004)

Category 4A7 Spam

#### 2004-05-20 CAN-SPAM law legislation volume statistics research

NWF http://www.nwfusion.com/news/2004/0520canslaw.html

CAN-SPAM CANNED?

By May 2004, it was clear that despite the CAN-SPAM Act, the volume of spam increased in the US in the first quarter of 2004. Spammers protested that when they tried to comply with the terms of the law, ISPs like AOL blocked their unwanted e-mail even more effectively. According to a report by Grant Gross in the IDG News Service, "Spammer Ronald Scelson, president of MicroEvolutions.com, told the committee he could go back to using forged headers and defeat most spam filters. 'Does the government want us to mail legal or not?' Scelson asked. 'As long as we're doing it the right way and we're going to get blocked, interfered with and shut down, people are going to go around it.' "

Category 4A7	Spam
2004-05-26	ban spam false subject lines e-mail Florida state message idea

NewsScan

FLORIDA LAW BANS DECEPTIVE SUBJECT LINES IN E-MAIL

Legislation signed by Florida Governor Jeb Bush will allow the state's attorney general to bring civil action against anyone in Florida who sends spam e-mail with a subject line intended to give the message recipient a false idea of what the message is about. (AP/USA Today 26 May 2004

## Category4A7Spam2004-05-31spam lawsuits investigations tracing money fraud law enforcement industry<br/>cooperation

http://www.nytimes.com/2004/05/31/technology/31spam.html?th=&pagewanted =print&position=

The fight again spam is increasingly involving traditional law enforcement investigation techniques. Because technological solutions have not yet stemmed the fetid tide of electronic slime, private investigators and police officers have been responding to spam advertisements and then tracking the money to arrest the perpetrators of scams and spam. According to Saul Hansell, writing in the New York Times, "...[T]he Direct Marketing Association has paid \$500,000 to hire 15 investigators who work alongside agents from the F.B.I. and other government agencies in a program known as Project Slam-Spam.... The project has built cases against 50 spammers, which it has started to refer to federal and state prosecutors. It hopes to orchestrate a coordinated sweep of spam prosecutions and civil cases later this year to highlight the seriousness of its antispam efforts."

Category 4A7 Spam

#### 2004-11-05 spam guilty Virginia sentencing AOL prosecution trial Jaynes DeGroot fraud

NewsScan; http://apnews.excite.com/article/20041105/D865NE501.html

SPAMMERS FACE CRIMINAL PENALTIES IN VIRGINIA TRIAL

Virginia prosecutors have brought to trial three North Carolina defendants in what's being billed as the nation's first felony antispam case. The Virginia law toughening penalties for sending junk e-mail took effect last year; if convicted, each defendant could face up to 15 years in prison and \$2,500 in fines. The prosecutors allege the defendants used falsified or forged return Internet addresses to send bulk e-mail hawking penny stocks and work-at-home schemes through a server in Loudon County, Virginia, where America Online is headquartered. The defense attorneys have argued their clients were simply "marketing via the Internet," which "may be annoying to you. It is not a crime." However, anti-spam activists say the prosecution is a step in the right direction. Spammers "are folks who are fairly comfortable with playing ... on the fringes of legitimacy and reality," says the general counsel for the Coalition Against Unsolicited Commercial E-mail. "But if you can attach serious jail time, they would think twice." (Washington Post 27 Oct 2004)

http://www.washingtonpost.com/wp-dyn/articles/A611-2004Oct26.html

\* \* \*

SPAMMERS GUILTY, MAY DRAW JAIL TIME

A brother-sister duo accused in Virginia of sending junk e-mail to millions of AOL customers were convicted yesterday in the first felony prosecution of Internet spam in the U.S. Jurors recommended that Jeremy Jaynes, 30, be sentenced to nine years in prison and his sister, Jessica DeGroot, 28, be fined \$7,500 after convicting them of three counts each of sending e-mail with fraudulent and untraceable routing information. A third defendant, Richard Rutkowski, 30, was acquitted. The case was the first to be brought under a tough Virginia anti-spam law that took effect last year. (AP 5 Nov 2004)

## 4A8 Liability

Category 4A8

Liability

hacking liability companies protect consumer data security privacy e-commerce

2004-03-04 NewsScan

SHIELDING AGAINST LIABILITY FOR HACKED DATA

Companies that handle consumer transactions typically require customers to agree to lengthy "terms-of-use" agreements in they waive any right to sue the company if its computers have been broken into by vandals. Consumer advocates say companies should be held accountable, and Chris Jay Hoofnagle of the Electronic Privacy Information Center argues that if companies are willing to derive the benefit of information collection they should accept the responsibility to secure it. But Verizon Wireless general counsel offers the corporate view that terms-of-use clauses are nothing more than good business practice and are not attempts to avoid corporate responsibility: "Verizon Wireless is very concerned with customer security and privacy. But we are trying to be fiscally responsible to protect the company from lawsuits." (Washington Post 4 Mar 2004)

## 4A9 Violent video games

Category 4A9 Violent video games

2004-12-16 Illinnois videogames crime rental sell

NewsScan; http://www.latimes.com/technology/la-na-videogame16dec16

ILLINOIS LEGISLATION TO REGULATE OVER-THE-TOP VIDEOGAMES

Illinois may be the first state in the country to regulate the sale and rental of violent and "adult" videogames, including ones such as "Grand Theft Auto: San Andreas," where players kill cops, steal cars, solicit prostitutes and then beat them to get their money back. Two bills being promoted by Illinois Gov. Rod Blagojevich would make it a crime for retailers to rent or sell such violent or sexually graphic material to minors. The videogame industry seems ready to shrug off the governor's proposals, and a spokesman for the Video Software Dealers Association says, "Every time there's a major new release, or a new release of technology, you see new attempts to regulate this industry." (Los Angeles Times 16 Dec 2004)

## 4B1 Copyrights

Category4B1Copyrights2004-01-08intellectual property rights violations South Korea US warm

NewsScan

U.S. WARNS SOUTH KOREA ON INTELLECTUAL PROPERTY VIOLATIONS

The Bush Administration is warning South Korea that it's not doing enough to stop the pirating of U.S. movies and music; U.S. Trade Representative Robert B. Zoellick says: "The pirating of U.S. intellectual property robs Americans and hurts those countries whose economies rely on innovation, technology and investment. Open markets and the protection of intellectual property are critical to the continued growth of our economy, and we'll vigorously press our trading partners to follow the rules." The South Korean response to the complaint was that the U.S. action was "very disappointing and regrettable." An executive of the Recording Industry Association of America (RIAA) says: "Online piracy of recorded music is rampant in Korea and has had a devastating impact on our industry already, significantly decreasing sales for international and local repertoire alike. Incomprehensibly, Korea has thus refused to provide the legal tools necessary for the recording industry to fight back." (Washington Post 8 Jan 2004)

Category 4B1	Copyrights
2004-02-26	EFF digital music intellectual property rights copyright RIAA download free music

NewsScan

FREE THE MUSIC

The Electronic Frontier Foundation is proposing legalization of online file-sharing through a voluntary music license that would compensate artists. EFF lawyer Fred von Lohmann says: "Everyone agrees that file-sharing does a better job distributing music than anything else out there. It gives people a much broader selection of software to choose from. And, of course, it's better-priced. The problem is that artists and copyright holders aren't being compensated." But music industry people say the EFF plan has little chance of success without the support of the major music labels, and Mitch Glazier of the Recording Industry Association of America (RIAA) says: "We've got a new, dynamic marketplace with Napster announcing its 5 millionth download. ITunes is just starting to get corporate partners. That's not failure at all. That's experimentation. Why the government should come in and take over a marketplace that's starting to develop is conceptually flawed in my mind." Wayne Rosso of the company that created Blubster and Piolet file-swapping services says: "I think it's one of several solutions that all reasonable men could probably understand and accept. The only problem is we're not dealing with reasonable men." (San Jose Mercury News 26 Feb 2004)

Category 4B1 Copyrights

#### 2004-03-01 copyright intellectual property rights issues digital report laws innovation

NewsScan

MEMO TO COPYRIGHT ENFORCERS: SLOW DOWN, TAKE A BREATH

A report from the policy group called Committee for Economic Development warns against efforts to support copyrights by preventing digital TV from being transmitted online. Called "Promoting Innovation and Economic Growth: The Special Problems of Digital Intellectual Property," the report concludes: "We are sympathetic to the problems confronting the content distribution industry. But these problems — perfect copies of high-value digital works being transmitted instantly around the world at almost no cost — require clear, concentrated thinking, rather than quick legislative or regulatory action." Not everyone is likely to agree with that recommendation. Jack Valenti, the president of the Motion Picture Association of America, has been highly critical of the notion that his industry is trying to place unfair burdens on consumers. "They say it will stifle innovation — that's malarkey. If all of this digital property is free, who is going to invest 50 to 60 million dollars to make a movie?" The report from the Committee for Economic Development has called for a two-year moratorium on changes to copyright laws and regulations: "Our first concern should be to 'do no harm.'" (New York Times 1 Mar 2004)

## Category 4B1 Copyrights 2004-05-03 microsoft DRM digital rights management software songs movies portable players expire

NewsScan

MICROSOFT'S NEW COPYRIGHT-PROTECTION SOFTWARE

Microsoft is introducing DRM "digital rights management" software software to allow rented songs or movies to be used on portable players, cellular phones and other devices. Songs and videos purchased through subscription services will be given digital expiration dates. The Walt Disney Co. and other companies are interested in using the new technology for their content. (Los Angeles Times 3 May 2004)

Category 4B1	Copyrights
2004-05-12	copyright act congress Digital Millennium Act DVD CD locks
NL C	

NewsScan

CONGRESS REVISITS 'FAIR USE' RESTRICTIONS IN COPYRIGHT ACT

A House subcommittee on consumer protection heard arguments yesterday on proposed amendments to the 1998 Digital Millennium Copyright Act, which imposed broad restrictions on bypassing technological "locks" on DVDs and some music CDs and software programs. The amendments, sponsored by Rick Boucher (D-Va.) and John Doolittle (R-Calif.), would reinstate the provision for "fair use" of such materials, even if circumvention of copy-protection software were necessary for such use. The sale of pirated DVDs and other forms of copyright infringement would remain illegal. "Without a change in the existing law, individuals will be less willing to purchase digital media if their use of the media within the home is severely circumscribed," says Boucher. "In addition, manufacturers of equipment and software which enable circumvention for legitimate purposes will be reluctant to introduce the products into the market." It's unclear whether the Boucher-Doolittle bill has much momentum behind it — so far, it has only 15 co-sponsors in the House, and there is no companion Senate bill as yet. (CNet News.com 12 May 2004)

#### Category 4B1 Copyrights

### 2004-06-23 copyright infringement intellectual property rights illegal file-swapping Senate broad law proposal

NewsScan

FRIST AND DASCHLE UNITE AGAINST ILLEGAL FILE-SWAPPING

Senate majority leader Bill Frist and minority leader Tom Daschle have joined up in attack against online music and video filesharing services and have co-introduced legislation to make anyone who "induces" illegal copying just as liable for breaking copyright law as the person who makes the copies. Wayne State University law professor Jessica D. Litman says she finds the bill "sort of scary" because it's "worded so broadly" and could be used against devices and technologies that have non-infringing as well as infringing uses, and Gary Shapiro of the Consumer Electronics Association says: "The VCR would not be a legal product; TiVo would not be a legal

product. I'm surprised the leadership would jump on this bill without hearing from the other side." But Emery Simon of the Business Software Alliance argues that such legislation is needed: "We have a huge piracy problem. Current law makes it difficult" to go after all the infractions." (Washington Post 23 Jun 2004)

## Category 4B1 Copyrights 2004-07-01 internet service provider ISP Canada Supreme Court lawsuit litigation copyright law infringement intellectual property rights jurisdiction

NewsScan

ISPs WIN MUSIC DOWNLOAD CASE

Canada's Supreme Court has ruled 9-0 that Internet service providers do not have to pay royalties to composers and artists for music downloaded by Web customers, since companies providing wide access to the Web are merely "intermediaries" who aren't bound by Canadian copyright legislation. At issue was an effort by the Society of Composers, Authors and Music Publishers of Canada (SOCAN) to force Internet service providers to pay a tariff. SOCAN also wanted to extend Canadian copyright law beyond the country's borders and apply it to offshore Web sites that serve Canadians. Opposing the effort was the Canadian Association of Internet Service Providers. (The Australian 1 Jul 2004) Rec'd from John Lamp, Deakin U.

## Category 4B1 Copyrights 2004-08-05 source code stolen Jolly Inc. Mumbai intellectual property rights outsourcing concern

#### DHS IAIP Daily;

http://www.computerworld.com/governmenttopics/government/legalissues/story/0,10801,95045,00.html

August 05, IDG News Service — Source code stolen from U.S. software company in India.

Jolly Technologies, a division of U.S. company Jolly Inc., reported Wednesday, August 4, that an insider at its research and development center in Mumbai, India, stole portions of the source code and confidential design documents relating to one of its key products. As a result, the company has halted all development at the center. A recently hired software engineer used her Yahoo e- mail account to upload and ship the copied files out of the research facility. Most U.S.- based software companies require their employees to sign an employment agreement that prohibits them from carrying the company's source code out of a development facility or transferring it in any way. Though the Indian branch of Jolly Technologies requires employees to sign a similar employment agreement, the sluggish Indian legal system and the absence of intellectual property laws make it nearly impossible to enforce such agreements, the company said.

## Category 4B1 Copyrights 2004-08-12 Nowergian hacker Jon Lech Johansen DVD-Jon iTunes encryption crack posting Website copyright infringement proprietary software

NewsScan

HACKER WANTS TO MAKE ITUNES EVERYBODY'S TUNES

Jon Lech Johansen, the Norwegian hacker who gained notoriety for developing DVD encryption-cracking software, has created a software key that unlocks the encryption Apple uses for its AirPort Express -- which lets users broadcast digital music from Apple's online iTunes Music Store on a

stereo not plugged into a computer. Johansen, who posted the key on his Web site (mockingly named "So Sue Me"), is an open source advocate critical of Apple for using a proprietary system to ensure that its products work only with each other. Apple has not yet reacted to this new intrusion. (AP/San Jose Mercury News 12 Aug 2004)

## Category 4B1 Copyrights 2004-08-25 copyright bill changes proposed legislation intellectual property rights file-sharing pressure

NewsScan

CHANGES TO NEW COPYRIGHT BILL URGED

The Consumer Electronics Association and the American Library Association, along with other technology and consumer groups, have recommended changes to the controversial Inducing Infringement of Copyrights Act (SB 2560), which is intended to discourage illegal file-sharing. The bill, sponsored by Sens. Orrin Hatch (R-Utah) and Patrick Leahy (D-Vt.), is supported by the record labels and Hollywood studios, who complain that illegal file-sharing is ruining their livelihood. But consumer groups recommend amending the legislation so "only someone who distributes a commercial computer program that is 'specifically designed' for wide-scale piracy on digital networks would be held liable for copyright violations," according to a press release. The proposed change would absolve ISPs, venture capitalists, credit card companies, banks, advertising agencies, IT help desks and librarians from liability. Emily Sheketoff, executive director of the American Library Association's Washington office, says she worries that SB 2560 "will quash innovation and

creativity and the fair use of these technologies. The answer to protecting copyright is not to stop developing new technologies. The answer is to educate people on how to use these technologies properly and encourage people to use these technologies properly. There are many legal, legitimate

file-sharing activities." (Wired.com 25 Aug 2004)

## Category4B1Copyrights2004-10-12P2P peer-to-peer supreme court

NewsScan; http://www.nytimes.com/2004/10/12/technology/12share.html

HOLLYWOOD PETITIONS SUPREME COURT ON FILE-SHARING

The entertainment industry is fighting back against peer-to-peer (P2P) file-sharing, petitioning the U.S. Supreme Court to overturn a federal appeals court decision reached in August that upheld file-sharing companies' right to distribute their software regardless of whether that software is later used to violate copyrights. That decision drew heavily on the precedent established by the 1984 Sony-Betamax case, which gave electronic device makers legal protection against claims of copyright infringement. This latest petition, which targets P2P purveyors Grokster and Streamcast Networks, cites a conflicting ruling reached in 2003, which upheld an injunction against P2P service Aimster on the grounds that it facilitated copyright infringement. However, critics say even the Aimster case upheld the basic tenets of the Sony-Betamax case. "They want to argue that there's some sort of national emergency here. But Betamax is the law of the land and it's not undermined by either of these two decisions," says Susan Crawford, a professor of Internet law at Cardozo School of Law in New York.

Category 4B1 Copyrights

#### 2004-10-20 music industry business model copyright Waldfogel strategy

NewsScan;

http://knowledge.wharton.upenn.edu/index.cfm?fa=viewArticle&id=1066

MUSIC INDUSTRY ON THE WRONG COURSE

Wharton business professor Joel Waldfogel says the music industry is mistakenly pursuing a short-term strategy in backing the Inducing Infringement of Copyrights Act of 2004, which would hold liable any entity that "intentionally aids, abets, induces or procures" copyrighted material. Rather than fighting technological advances through litigation, the music industry must come up with new business models -- for instance, taking advantage of the Internet to slash its distribution costs. "Instead of putting out CDs and shipping them on trucks, they can send them directly at a very low cost. That does suggest a very different business model than charging \$15 or \$20 for a CD. It might be a much more attractive way to do things. Stuff that is easy to distribute wants to be free. Given that force, I think [the recording industry] needs to come up with a new model for generating income," says Waldfogel. (Knowledge@Wharton Oct 20-Nov 2 2004)

Category 4B1 Copyrights

2004-10-31 venture capital Internet music

NewsScan;

 $http://news.com.com/iTunes+aside\%2C+Web+is+changing+the+music+industry/2100-1027\_3-5433891.html$ 

INTERNET MUSIC REWRITES INDUSTRY RULES

While the music industry has been focusing on music piracy, another phenomenon is slowly emerging -- the Web as venture capital source. Chart-topping rockers The Darkness have sold enough downloads, T-shirts and other fan-abilia to finance their next album, and British band Marillion has used its site to raise funds for its last two albums -- before they recorded them. "The Internet is our savior. Without it, we wouldn't be what we are today. It's really turned the business around," says Marillion's marketing manager. Meanwhile, Universal Music has begun using the Web as a testing/breeding ground for new acts, signing them to a "digital rights" contract before committing serious money to their promotion. "It acts as an incubation label, if you will," says Universal Music UK new media services director Rob Wells. "It's the Marillion concept." (Reuters/CNet 31 Oct 2004)

Category 4B1 Copyrights

#### 2004-11-15 music Napster Snocap Universal P2P peer-to-peer

NewsScan; http://online.wsj.com/article/0

UNIVERSAL AND SNOCAP MAKE MUSIC TOGETHER

Vivendi Universal has agreed to license its catalog of 150,000 songs to Snocap, a new venture headed up by Napster founder Shawn Fanning. It's unclear how Snocap's peer-to-peer service will work, but people close to the deal say one possibility is that the service would allow users to share a low-quality copy of a licensed song for free but would require a fee for access to a highquality version. The other three big labels -- Warner Music, EMI Group and Sony BMG -- all are seeking ways to license legitimate copies of their songs to peer-to-peer network, but Universal's move marks the first such partnering deal. (Wall Street Journal 15 Nov 2004)

### Category 4B1 Copyrights

2004-12-16 copyright music Hatch MPAA Specter politics

NewsScan; http://www.washingtonpost.com/wp-dyn/articles/A4003-2004Dec16.html

WHAT PROSPECT FOR CHANGE IN COPYRIGHT POLICY?

On the issue of protecting music and movies from Internet piracy, Senator Orrin Hatch (R, UT), a songwriter himself, has been the entertainment industry's most powerful ally in Congress, but in 2005 Sen. Arlen Specter (R, PA) will replace Hatch as chairman of the Senate Judiciary Committee. Will there be much change? One aide says that Specter "has been a follower rather than a leader on these issues" and therefore might let Hatch keep holding the reins. However, David Green of the Motion Picture Association of America (MPAA) predicts that Specter will rise to the occasion: "Copyright issues are important and they're going to percolate up, and it's really impossible for him to ignore them. He might be right now more interested in something else, but because these issues are important to America they are going to be important to Arlen Specter." (Washington Post 16 Dec 2004)

### 4B2 Patents

Category4B2Patents2004-01-12patent infringement lawsuit Rockwell automation customersRISKS; http://www.law.com/jsp/article.jsp?id=103905447880023SUING THE CUSTOMERS

Joyce Scrivner writes about a patent infringement countersuit by Rockwell Automation Inc. Rockwell was suing "a law firm currently suing Rockwell's customers." Rockwell customers were being sued because they could potentially cough up more money than Rockwell itself. Rockwell feels that the law firm, Niro Scavone, sought to "shakedown' manufacturers through threats of potential business interruption or catastrophic damages." In a follow-up article, contributor Paul Robinson comments that Rockwell automation "doesn't have a leg to stand on" in this case. According to patent law, he says, everyone in the chain of producer, distributor, and consumer is liable if they've been in contact with a product that infringes on someone else's patent. It doesn't matter who is actually sued. Robinson adds that Rockwell is wrong to call Niro Scavone's actions a 'shakedown' because the law firm was "using the courts." He explains: "If I threaten you if you don't pay me for something, that's extortion and a crime. If I threaten to sue you if you don't settle, that's legal. If I just sue you anyway, whether I have a case or not, that's also legal."

Category 4B2	Patents
2004-01-13	US patent system obsolete

NewsScan

PATENTLY ABSURD?

A number of industry and government officials have come to the conclusion that the U.S. patent system has become absurd — especially in fields such as computers, software and biotechnology. Intellectual property attorney Mark Banner says: "Very bad patents are getting through. It's draining millions of dollars that could be spent on finding a better mousetrap." Yet the current system has its defenders. Jon Dudas of the Patent Office insists that most patents are valid, and Jay Walker (whose company patented the "reverse auction") argues: "We as a nation are ahead of the rest of the world because we have strong property rights. Everybody said you couldn't have patents on electricity. Guess what? They were wrong." Others in the debate take the position that the problem with the patent system is not that it's unfair but that it's irrelevant: software executive Jordan Greenhall says: "If you didn't have any patents at all, people would still be doing the same stuff because of the speed of the marketplace." (USA Today 13 Jan 2004)

Category 4B2 Patents

#### 2004-03-02 Toshiba flash memory intellectual property rights issues patents licences

NewsScan

TOSHIBA ENGINEER SUES FOR 20% OF FLASH MEMORY PROFITS

A former Toshiba engineer is suing his former employer, the Japanese electronics maker, alleging that he was insufficiently compensated for his work developing flash memory technology. That technology has made 20 billion yen (US\$183.49 million) in profits for Toshiba, and the engineer, who now a university professor, is asserting that his fair share of those profits is 20%. Flash memory chips, which are able to retain data after power is switched off, are widely used in mobile phones, digital cameras and other portable electronics.(San Jose Mercury News 2 Mar 2004)

12

#### Category 4B2 Patents

2004-03-05 intellectual property rights patents Internet Explorer browser Microsoft infringement

NewsScan

PTO REJECTS EOLAS PATENT CLAIM

In a move that could cripple their lawsuit against Microsoft, the U.S. Patent and Trademark Office has reached a preliminary decision to invalidate Eolas Technologies' and the University of California's patent on Web browser technology. Eolas and UC had won a \$521 million verdict against Microsoft last year for infringing on their patent in its Internet Explorer browser, a decision that was upheld last month by an Illinois federal judge. The software giant had already started to make changes to Internet Explorer to comply with the court's ruling, but suspended those changes last month in hope of a reprieve by the PTO. "We have maintained all along that, when scrutinized closely, this patent would be ruled invalid," said a Microsoft spokesman. Meanwhile, Eolas attorney Martin Lueck said it was not uncommon for the PTO to invalidate a patent claim as the first step in the review process and remained upbeat about the final outcome of the litigation. (Reuters/CNet News.com 5 Mar 2004)

Category 4B2	Patents
2004-03-17	intellectual property rights ownership Kazaa source code

NewsScan

KAZAA RHUMBA

Fabian Toader, a programmer in Redmond, Washington, claims he wrote the source code for the Kazaa file-sharing software while he was a freelancer in his native Romania, and he is now suing the program's distributor, Sharman Networks, for \$25 million in compensation. Toader says, "Sharman has made millions using my software. I just want to be fairly compensated for my contribution." Sharma, whose home offices are in Sydney, Australia, says: "The work done by Fabian Toader on early versions of the Kazaa Media Desktop software was done under a work for hire agreement that expressly states that Kazaa B.V. owned all rights to any work related to the development of the software." A Sharman spokesman has called Toader's new lawsuit a "shakedown effort." (AP/USA Today 17 Mar 2004)

Category 4B2	Patents			
00010110		 	·· ··*	-

2004-04-12 intellectual property digital rights management patents lawsuit settlement

NewsScan

MICROSOFT SETTLES INTERTRUST PATENT LAWSUIT

Microsoft has settled a lawsuit brought three years ago by InterTrust Technologies, which alleged that the software giant infringed on its digital rights management patents. Microsoft will pay \$440 million to InterTrust, which is owned by a joint venture of Sony, Philips Electronics and investment banking firm Stephens Inc. The announcement comes on the heels of Microsoft's agreement last week to pay Sun Microsystems \$1.6 million to settle an antitrust lawsuit and resolve patent claims. And last month, Microsoft settled a patent lawsuit filed by AT&T over voice-recognition technology. Terms of that settlement were not disclosed. (AP/Washington Post 12 Apr 2004)

Category 4B2	Patents
2004-08-09	patent licensing demand Acacia academia intellectual property rights

NewsScan

#### ACACIA PRESSURES ACADEMIA FOR PATENT PAYMENTS

Acacia Media Technologies, which last month suffered a setback in its efforts to force adult entertainment sites to make licensing payments for using its patented streaming video technology, has now turned its attention to higher education, whipping off dozens of letters to colleges claiming

the schools' use of streaming video for purposes such as distance learning violates its patents. Acacia's digital media patents were acquired from Greenwich Information Technologies in 2001 and since then Acacia has secured dozens of licensing deals with companies, including Walt Disney.

And while a handful of colleges and universities have agreed to pay up, most have resisted. The American Council on Education and the Electronic Frontier Foundation both are advising colleges not to pay, citing last month's legal ruling that several terms in Acacia's patents were indefinite

-- a verdict that could knock a hole in Acacia's case for demanding payments from other sectors. "Honestly, I think it's a sign of desperation," says EFF staff attorney Jason Schultz. "Acacia knows the hammer is coming down on its patents, and it's going to extract as much as it can before the apocalypse," adding that the company's tactics were "a threat to the future of education... I think that's despicable. Universities are under enough pressure in their budgets right now to try to pay for everything. The last thing they need to do is give a pound of flesh to some tech company that doesn't even make a product." (AP 9 Aug 2004)

Category 4B2 Patents

#### 2004-10-01 patents Microsoft open source FAT file allocation table appeal

NewsScan; http://www.usatoday.com/tech/news/techpolicy/2004-10-01-fat-patent-rejected

MICROSOFT LOSES PATENT BATTLE

In a victory for "open source" advocates, the U.S. Patent and Trademark Office has rejected a Microsoft application for a patent on a system called File Allocation Table (FAT), which lets people create and find files on a computer using easy-to-remember names. The reason for the rejection is that the technology in question is already widely used throughout the industry. Independent patent expert Greg Aharonian comments: "It's like getting a patent on cheesecake." Microsoft plans to file an appeal.

Category 4B2 Patents

#### 2004-11-03 video games patent Electronic Arts Atari Sega McKool Smith

NewsScan; http://www.theregister.com/2004/11/03/game\_cos\_3d\_lawsuit/

GAME MAKERS THREATENED BY PATENT LAWSUIT

Computer game makers, including such big names as Electronic Arts, Atari and Sega, have been sued by Texas-based McKool Smith, which claims the makers' games violate a 1987 patent that covers a way to display 3D objects realistically in a 2D space, such as a computer monitor. The technique is used by almost every game that uses 3D modeling, including older games such as Quake and Doom. The companies are now frantically researching prior art, citing games such as The Colony and Spectre, which may have been released before the 1987 patent was granted. (The Register 3 Nov 2004)

Category 4B2 Patents

#### 2004-11-15 Microsoft Xbox modification cheating live multiuser games fraud

NewsScan; http://www.siliconvalley.com/mld/siliconvalley/10189248.htm

MICROSOFT CRACKS DOWN ON XBOX MODIFICATIONS

Cameron Ferroni, Microsoft's general manager for the Xbox software platform, says the company's not planning to sue individual users but that it does want to stop users of the Xbox Live online service from modifying their machines to improve their performance at games. Ferroni believes it's important that Microsoft prevent cheating on Xbox Live (where multiple players can take part in games) and says that the company's goal is to make sure there's a level playing field for game players. (AP/San Jose Mercury News 15 Nov 2004)

### 4B3 Reverse engineering

Category 4B3 Reverse engineering

#### 2004-10-04 reverse engineering genome algorithms protocols computer science

NewsScan; http://www.wired.com/news/infostructure/0

REVERSE ENGINEERING TAKES A LESSON FROM THE GENOME PROJECT

There's a lot more in common between reverse-engineering software and the algorithms used in bioinformatics research than you would expect, says security analyst Marshall Beddoe. In both cases, scientists must fill in a lot of blanks -- much of bioinformatics is devoted to finding DNA sequences separated by long gaps of unknown data, and the same is true in protocol reverse-engineering. Scientists attempting to reverse engineer software protocols find that network conversations are full of "junk" -- usually the actual data being sent -- which interferes with the analysis of the of the command sequences. Beddoe solved the problem by using bioinformatics algorithms to eliminate the junk data sandwiched between commands. Meanwhile, Avaya senior security consultant Dan Kaminsky says he's investigating using genomic pattern analysis for identifying and clustering "mutant" machines on a corporate network. "Generating an ordered, hierarchical breakdown of interrelationships from huge piles of information is a problem that crops up everywhere. I'm not surprised to see bioinformatics solutions finally being applied to the rest of our poorly understood, oversized networks," says Kaminsky.

Category 4B3 Reverse engineering

2004-12-15 **iPod Apple RealNetworks Harmony music copy protection blocking information** warfare reverse engineering

NewsScan; http://www.siliconvalley.com/mld/siliconvalley/10425219.htm

ANOTHER ROUND IN THE APPLE-VS.-REAL NETWORKS FIGHT

Apple has begun blocking the technology that RealNetworks created to evade the copy-protection shield used by Apple's iPod. When RealNetworks introduced its Harmony technology this summer, it hoped to dissolve some of the barriers created by incompatible, proprietary digital music standards, and said it had reverse-engineered Apple's copy-protection code to allow songs purchased from non-Apple online outlets to be playable on the iPod. To deal with Apple's new move, RealNetworks now says it "will look at the Apple upgrade and see how it'll make Harmony work once again with the iPod." (AP/San Jose Mercury News 15 Dec 2004)

### 4B5 Trademarks

Category 4B5 Trademarks

#### Apple loses trademark appeal China logo clothing hats shoes

2004-06-22 NewsScan

APPLE LOSES APPEAL AGAINST TRADEMARK PANEL DECISION

Apple has lost a court appeal against a decision that rejected its request to have its trademark logo extended to cover clothing and other items in China. The verdict by the Beijing No.1 Intermediate People's Court means that Apple cannot claim that its logo is protected under law for those goods. The trademark appraisal committee of China's State Administration for Industry and Commerce had previously rejected Apple's application from April 2000 to have its trademark logo extended to cover clothing, hats and shoes. Guangdong Apples Industrial Co, a Chinese maker of leather goods, had registered a similar trademark with an entire apple, while Apple Computer's

trademark has an apple with a bite taken out of it. (The Age 22 Jun 2004)

### Category 4B5 Trademarks

2004-07-19 Lindows Microsoft Windowd trademark copyright out-of-court settlement

NewsScan

LINDOWS INSPIRED TO CHANGE ITS NAME FOR \$20 MILLION

Microsoft has settled its trademark infringement lawsuits against Lindows with a \$20 million payment to that Linux operating system company -- which will now change its name to Linspire. Microsoft says, "We are pleased that Lindows will now compete in the market place with a name distinctly its own." Lindows has four years to continue using two of its Web addresses <a href="https://www.lindows.com">www.lindows.com</a> of redirecting visitors to its new Web sites. (AP/USA Today 19 Jul 2004)

#### Category 4B5 Trademarks

#### 2004-08-15 USPS personalized individualized stamps Stamps.com order

NewsScan

USPS AUTHORIZES INDIVIDUALIZED STAMPS

The U.S. Postal Service has put its stamp of approval on Stamps.com's plans to test a new service (www.photo.stamps.com) that enables users to design their own legally valid stamps using digitized photos of their pets, children or almost anything else that strikes their fancy. (Stamps.com says

it will screen each photo submission to weed out objectionable material such as nudity, obscenity, politics, violence and trademark infringements.) The personalized stamps don't come cheap -- at \$16.99 for a minimum order of 20 37-cent stamps they cost 85 cents apiece -- but Stamps.com CEO Ken McBride reports that more than 2,000 sheets of personal stamps were ordered in the first two days and he anticipates the trial will win approval from the USPS and will be extended. (Washington Post 15 Aug 2004)

#### Category 4B5 Trademarks

#### 2004-12-15 Geico Google law dismissed trademark search engines advertising paid links

NewsScan; http://www.nytimes.com/2004/12/15/technology/15cndroogle.html?orof\_login

google.html?oref=login

GEICO CASE AGAINST GOOGLE DISMISSED BY JUDGE

A federal district court judge in Virginia has dismissed a key claim in the trademark infringement suit brought against Google by Geico, the auto insurance company. Geico had argued that the Google practice that allows Geico's competitors to buy ads linked to searches for "Geico" and "Geico Direct" confuses Web surfers who are looking specifically for Geico, but the judge ruled that there was not enough evidence the Google practice actually confuses consumers. One intellectual property attorney not involved in the case predicts: "It will not be binding precedent. That's how cases get to the Supreme Court." (New York Times 15 Dec 2004)

### 4C1 Paradigms, security standards

Category 4C1 Paradigms, security standards

2004-01-15 monoculture SNMP virus worm network Internet parallel agriculture pest epidemic

CNET News http://news.com.com/Seeds+of+destruction/2009-7349\_3-5140971.html

AGRICULTURE EPIDEMICS MAY HOLD CLUES TO NET VIRUSES

Computer scientists and biologists have been thinking about the parallels between computer viruses and biological viruses for years. Robert Lemos, a distinguished writer for CNET News, wrote a report on the growing collaboration in January 2004. One of the main ideas is that monoculture makes both agricultural fields and computer networks more susceptible to pathogens such as the Potato Blight that devastated Ireland in 1845 and the MSBlast worm that attacked Windows computers in August 2003. Many experts have pointed out that almost all of the major attacks on the Internet have been rooted in the Microsoft monoculture, including the Outlook e-mail client and the IIS (Internet Information Server) products. Another widespread technology at risk is SNMP, which could also be exploited by worms.

Category 4C1	Paradigms, security standards
2004-01-22	Common Criteria CC certification standard Linux SUSE Enterprise Server 8 IBM eServer Access Protection Profile

NIPC/DHS

LinuxWorld: SuSE, IBM gain higher security certification

Raising the security bar one notch higher, SuSE Linux AG and IBM Wednesday said they have achieved a more rigorous security certification for Linux operating system software running on Big Blue servers. With the higher-level security evaluation, the two companies hope to attract governments and organizations with critical operations to open source Linux software.

Category 4C1 Paradigms, security standards

#### 2004-01-26 NIST IT security draft report guidelines

NIPC/DHS; ;

http://www.fcw.com/fcw/articles/2004/0119/web-nist-01-23-04.asp

January 23, Federal Computer Week — NIST releases telnet, IT security drafts.

Federal agencies desiring to minimize work disruptions from outside intrusions can begin with simple safeguards, such as preventing unauthorized users from using the telnet protocol to gain access to a server, according to officials at the National Institute of Standards and Technology (NIST). Draft documents on computer security released Thursday, January 22, by the NIST give an example of how unauthorized telnet users simply identify themselves as a guest to gain access to sensitive government files. The Risk Management Guide for Information Technology Systems suggests that disabling telnet is about a 10-hour procedure. Practical advice in the 58-page document includes other ways that agencies can develop standards for safeguarding sensitive but unclassified information in federal computer systems. As applied to information systems, the guide says, risk management is a responsibility of executive managers to be shared with technical managers, and not a technical manager's sole responsibility. Engineering Principles for Information Technology Security, a 33-page document also released this week, offers an overview of accepted principles and practices for security information technology systems. Additional information can be found on the NIST Website:

http://csrc.nist.gov/publications/drafts.html

Category 4	C1	Paradigms,	security standards
------------	----	------------	--------------------

2004-02-14 Common Criteria CC certification standard Pointsec Mobile Level 4 EAL5 PC hard disk encryption software

NIPC/DHS

Pointsec Gains CC Certification For Encryption Software

Pointsec Mobile Technologies says it has gained Evaluation Level 4 (EAL4) Common Criteria certification for its Pointsec for PC hard disk encryption software The SC Infosecurity Newswire, Feb 13, 2004. Category4C1Paradigms, security standards2004-02-23AVDL Application Vulnerability Description Language XML base standard security

DHS IAIP Daily; http://www.informationweek.com/story/showArticle.jhtml?artic leID=18100080

February 23, Information Week — Application security standard edges forward.

An application security standard known as Application Vulnerability Description Language (AVDL), which was proposed last year, is moving closer to reality. AVDL is based on XML and is designed to provide a standard way for application vulnerabilities to be defined and classified so all security applications from different vendors that companies use to secure their apps will understand the same language when it comes to security threats. For example, when a new software vulnerability surfaces, a company's vulnerability scanner could scan systems to spot the new flaw. The scanner then could send information to firewalls and patch- management systems, which those applications could then use to automatically adjust to better protect against any potential attacks, such as a worm or a hacker attack. AVDL 1.0 standard is complete and is expected to receive final standards approval next month. Gartner VP and analyst John Pescatore says that because of the number of application vulnerabilities that surface each week - - sometimes more than 80 are announced - - standards such as AVDL can help companies reduce the threat they face from the moment a vulnerability is discovered to the time it takes them to respond and patch.

Calegoly 4C1 Paradignis, security standards	Category	4C1	Paradigms, security standards
---	----------	-----	-------------------------------

#### 2004-04-01 NIST draft standards securing computer systems

DHS IAIP Daily; Source:

http://www.fcw.com/fcw/articles/2004/0329/web-nist-04-01-04.asp

April 01, Federal Computer Week — NIST releases drafts.

Officials at the National Institute of Standards and Technology (NIST) announced this week the draft release of two security documents that provide detailed guidelines to federal agencies and other organizations for securing computer information systems. Special Publication 800- 60, "Guide to Mapping Types of Information and Information Systems to Security Categories," is the second draft of a document meant to help federal agencies meet the requirements of the Federal Information Security Management Act of 2002. It describes how to categorize types of information and information systems for assessing security risks. Both documents are available at

http://csrc.nist.gov/publications/drafts.html. The publications complement previous technical works from NIST.

Category 4C1 Paradigms, security standards

#### 2004-04-06 NIST security standards guidelines draft online

DHS IAIP Daily;

http://fcw.com/fcw/articles/2004/0405/web- nist- 04- 06- 04.asp

April 06, Federal Computer week — Last draft released for security guide.

The National Institute of Standards and Technology (NIST) on April 6 released a final draft of security guidelines for federal agencies that need to certify and accredit their information systems. With May as their target date for publication, NIST officials cited an urgent need to receive comments on the final draft document by April 21. The proposed guidelines are relevant to security requirements that all federal agencies must meet under the Federal Information Security Management Act of 2002. NIST officials incorporated several significant changes in the final draft based on earlier comments they received. Among them are newly defined roles for the chief information officer and senior agency information security officer in the certification and accreditation process. Also new are additional guidelines for low- impact information systems, a revised timetable for interim approval to operate information systems, and a summary table of tasks and subtasks for security certification and accreditation. Special Publication 800- 37, Guide for the Security Certification and Accreditation of Federal Information Systems, is available online.

Category 4C1 Paradigms, security standards

### 2004-04-13 Common Criteria CC certification standard Apple Computer Mac OS X open-source government

NewsScan

APPLE PUSHES FEDS TOWARD BROADER OPEN-SOURCE USE

Apple Computer Inc. is seeking Common Criteria evaluation of Mac OS X, which could open government doors wider to open-source software.

## Category 4C1 Paradigms, security standards 2004-04-14 Common Criteria CC certification standard Symantec Firewall componenet Level 4 EAL4

SYMANTEC FIREWALL COMPONENT RECEIVES CERTIFICATION

The firewall engine of Symantec Corp.'s Gateway Security 5400 appliance has received Common Criteria Evaluation Assurance Level 4 certification.

Category 4C1	Paradigms, security standards
2004-04-19	cyber security strategy federal government recommendations

#### DHS IAIP Daily;

http://fcw.com/fcw/articles/2004/0419/web- ncsp- 04- 19- 04.asp

April 19, Federal Computer Week — Last part of security strategy released.

A cybersecurity task force organized by the National Cyber Security Partnership issued a 104- page report with recommendations for the federal government and industry on Monday, April 19. The report is the last of five documents prepared by industry and academic experts on the President's National Strategy to Secure Cyberspace, a general blueprint for improving the nation's cybersecurity readiness. The task force members called for what they said were needed improvements to the consumer- and vendor- oriented software security testing program operated by the National Institute of Standards and Technology and the National Security Agency. The report recommends that NIST receive an initial \$12 million in new appropriations and \$6 million in following years for developing security requirements for specific classes of products such as intrusion- detection systems and virtual private networks. Other steps outlined in the report include making vendors responsible for shipping software products with more of their security features enabled and having the federal government mandate software- vulnerability analysis as a condition of procurement. The group also recommended that industry groups work together to develop a well- defined set of technical standards for designing secure IP networks. The report is available online:

http://www.cyberpartnership.org/TF4TechReport.pdf

#### Category 4C1 Paradigms, security standards

#### 2004-04-29 security needs protecting company information assets Network Applications Consortium

DHS IAIP Daily; http://www.nwfusion.com/news/2004/0426nac.html

April 26, Network World — User group defines security needs.

The Network Applications Consortium (NAC) plans to publish a document this summer that outlines the principle, policies, standards, technologies and processes necessary to protect a company's information assets. NAC's Enterprise Security Architecture addresses hot topics in cybersecurity such as governance, technology architecture and operations. The document will affect how several major corporations- - including Bechtel, Boeing, GlaxoSmithKline and State Farm Insurance- - make network hardware and software purchases in the future, network executives at these companies say. NAC members also plan to use the document to influence how key network vendors such as Cisco, Entrust, Microsoft and Symantec create security products. The consortium plans to embrace several security standards- - selections have not been finalized- - and urge vendors to adopt these standards. The document's goal is to create a framework that lets companies mix and match security products from different vendors while assuring interoperability and manageability. Additional information is available on the NAC Website:

http://www.netapps.org/

Category 4	4C1	Paradigms.	security standards
------------	-----	------------	--------------------

#### 2004-05-09 Sasser german teenager \$250000 microsoft sabotage computer

NewsScan

SASSER CREATOR TURNED IN FOR THE REWARD

The German teenager who created the computer worm Sasser was identified by acquaintances seeking a \$250,000 reward from Microsoft. The young man was arrested in the village of Waffensen, near Bremen, and appeared shaken by the extent of the damage his program had caused around the world. He faces charges of computer sabotage, which under German law could mean his imprisonment for five years. If the teenager is convicted, Microsoft will make good on its pledge for the full \$250,000 reward. (Washington Post 9 May 2004)

### Category4C1Paradigms, security standards2004-05-13NIST Standards Documentation FISMA

DHS IAIP Daily; http://www.gcn.com/vol1\_no1/daily- updates/25881- 1.html

May 13, Government Computer News — NIST releases computer security documents.

The National Institute of Standards and Technology (NIST) has published final versions of three computer security documents and released one draft document for public comment. Special Publication 800- 38C, Recommendation for Block Cipher Modes of Operation: the CCM Mode for Authentication and Confidentiality, specifies an authenticated encryption mode of the Advanced Encryption Standard. The Guide for the Security Certification and Accreditation of Federal Information Systems (Special Publication 800- 37), is one of a series of guidelines to help agencies comply with the Federal Information Security Management Act (FISMA). FISMA requires that all IT systems be certified and accredited for operation. The new guidelines provide a standardized approach for assessing the effectiveness of security controls determining the risks posed by threats to the system. A draft of An Introductory Resource Guide for Implementation of the Health Insurance Portability and Accountability Act Security Rule (Special Publication 800- 66), provides help for agencies subject to both HIPPA and FISMA. The document identifies NIST resources for addressing HIPPA requirements, and provides cross- mapping between HIPPA and FISMA requirements to help agencies avoid redundant work. Additional information is available on the NIST Website: http://www.nist.gov/

Category 4C1	Paradigms, security standards
2004-05-24	cybersecurity corporate executives threats outside hackers inside jobs CSO Carnegie Mellon CERT

NewsScan

CORPORATE EXECS SHIFT THEIR FOCUS TO OUTSIDE CYBERTHREATS

A greater percentage of corporate executives are worried about cybersecurity threats from outside hackers than inside jobs by disgruntled or recently fired workers, according to a recent survey conducted by CSO (Chief Security Officer) magazine in cooperation with the Secret Service and Carnegie Mellon's CERT (Computer Emergency Response Team). The shift in focus marks a change in corporate attitudes toward security, says CSO publisher Robert Bragdon: "Historically, businesses have always focused on internal threats being the biggest dangers to their organization." But despite the change, 36% of the 500 executives polled said they still managed to keep a close eye on employees' Web activities and e-mail to prevent internal sabotage and leaks. Meanwhile, the costs of computer crime are going up. The study estimates that cybercrime attacks against businesses and government agencies cost \$666 million last year. (Washington Post 24 May 2004)

Category 4C1 Paradigms, security standards

#### 2004-05-25 vulnerability reporting OIS guidelines

DHS IAIP Daily; http://www.gcn.com/vol1\_no1/daily- updates/26045- 1.html

May 25, Government Computer News — Group wants input on vulnerability reporting guidelines.

The Organization for Internet Safety (OIS) is soliciting comments on its guidelines for reporting and responding to software security vulnerabilities. OIS, a consortium of software vendors, researchers and security consultants, released the guidelines in July 2003, hoping to bring some order to the continual struggle between code makers and code breakers. The second version is expected to be available in mid-July. OIS hopes to address some issues in the second release that were sidestepped in the first edition, such as what role—if any—the government should play in vulnerability reporting. The voluntary guidelines are an effort to balance the public's right to know about possible software problems against the need for vendors to correct those problems before they are made public. Comments are being accepted through June 24 at feedback@oisafety.org. Details for the comment process are available at www.oisafety.org/review- 1.5.html

# Category 4C1 Paradigms, security standards 2004-08-24 Microsoft leaves UN standards group Center Trade Facilitation Electronic Business intellectual property open source proprietary software

NewsScan

MICROSOFT BUGS OUT OF U.N. STANDARDS GROUP

Microsoft has withdrawn from a U.N. software standards group focused on automating buying and selling through networks of computers. The diverse membership of the group -- known as the United Nations Center for Trade Facilitation and Electronic Business (U.N./Cefact) -- includes advocates of both proprietary and open-source approaches to software technology standards; however, Microsoft-watchers believe that the company's decision to withdraw from the group can be traced not to the open-source vs. proprietary standards debate but rather to issues concerning control of the intellectual property being contributed to the standards-setting effort. (New York Times 24 Aug 2004)

Category 4C1	Paradigms, security standards
2004-10-27	National Information Assurance Partnership NAIP Common Criteria CC praise certification

DHS IAIP Daily;

http://www.fcw.com/fcw/articles/2004/1025/web- niap- 10- 27- 04. asp

October 27, Federal Computer Week — NIAP chief touts Common Criteria.

Officials at the National Information Assurance Partnership (NAIP) have effectively raised the level of security in many information technology products used by the government, the security group's director said Wednesday, October 27. NIAP, an initiative of the National Institute of Standards and Technology and the National Security Agency, is responsible for implementing the Common Criteria Evaluation and Validation Scheme, a rigorous set of security tests that adhere to international standards. The testing directly improved 30 percent of the products tested by eliminating security flaws that could have been exploited by attackers, said Jean Schaffer, director of NIAP. Critics say Common Criteria testing costs too much and takes too long, but Schaffer argued that these claims are made by those who do not have firsthand knowledge about the testing.

# 4C2 Risk management methodology & tools

#### NewsScan

STARTUP OFFERS INSURANCE AGAINST LINUX COPYRIGHT CLAIMS

Open Source Risk Management is launching insurance-like protection aimed at indemnifying Linux users against copyright infringement claims like those made by SCO Group. The company says it has completed a six-month study comparing Linux with several version of Unix and found no copyright problems. "We have come out of the examination process with the strong belief that there are no meritorious copyright infringement claims in the kernel. With all we have seen to date, I don't believe they have a strong case," says OSRM executive director John St. Clair. OSRM's legal protection covers only copyright infringement, but it plans to offer patent protection as well for an additional charge. It also has launched an Open Source Legal Defense Center, which offers companies expert legal advice for \$100,000 per year, while charging \$250 per year for individual programmers. The copyright-infringement protection is priced at 3% per year of the total coverage -- so for protection against \$1 million of legal costs, a company would pay \$30,000. Meanwhile, an SCO spokesman disputed OSRM's claims: "Everything we have looked at and found would run contrary to what they're finding." (CNet News.com 18 Apr 2004)

#### Category 4C2 Risk management methodology & tools

#### 2004-05-25 software suppliers risk management defense acquisitions

DHS IAIP Daily; http://www.gao.gov/new.items/d04678.pdf

May 25, General Accounting Office — GAO- 04- 678: Defense Acquisitions: Knowledge of Software Suppliers Needed to Manage Risks (Report).

The Department of Defense (DoD) is increasingly reliant on software and information systems for its weapon capabilities, and DoD prime contractors are subcontracting more of their software development. The increased reliance on software and a greater number of suppliers results in more opportunities to exploit vulnerabilities in defense software. In addition, DoD has reported that countries hostile to the United States are focusing resources on information warfare strategies. Therefore, software security, including the need for protection of software code from malicious activity, is an area of concern for many DoD programs. GAO was asked to examine DoD's efforts to (1) identify software development suppliers and (2) manage risks related to foreign involvement in software development on weapon systems. To address software vulnerabilities and threats, GAO recommends that DoD better define software security requirements and require program managers to mitigate associated risks accordingly. DoD agreed with the findings but only partially concurred with the recommendations over concerns that they place too much responsibility for risk mitigation with program managers. GAO has broadened the recommendations to address DoD's concerns. Highlights: http://www.gao.gov/highlights/d04678high.pdf

# 4C4 Professional certification in security, auditing

# Category4C4Professional certification in security, auditing2004-09-01information technology IT users United Kingdom UK IA security staff certification<br/>financial corporate auditing regulations

DHS IAIP Daily; http://www.computing.co.uk/news/1157762

September 01, Computing (UK) — IT users seek to certify security.

IT security experts from some of the UK's most influential businesses are meeting this week to try to establish a professional body for certifying information security staff. The group, which includes the Royal Bank of Scotland, Royal Mail and BP, will meet with The Information Security Forum, in an attempt to create an industry body which links financial and IT security needs. David Lacey, Royal Mail director of information security, told Computing that the group hopes to establish codes of conduct and professional certification for IT security staff, to ensure compliance with growing corporate financial auditing regulations. Following the meeting, the group will expand its plans for security standards, benchmarking, business processes and vendor management. Lacey expects to produce a report before the end of October to share with IT suppliers.

Category4C4Professional certification in security, auditing2004-10-18certification Australia ACS accreditation agency IT profession mandatory<br/>membership

NewsScan; http://australianit.news.com.au/articles/0

ACS PUSHES OWN IT 'LICENSE'

The Australian Computer Society (ACS) has called on government to support its bid to become the accreditation agency for the IT profession, making membership mandatory for computer staffers ranging from Microsoft Certified Engineers to high-level project managers. ACS president Edward Mandla also called for state and federal governments to assist in funding Australian companies seeking to acquire quality assurance certification like CMMI and ISO 15504. Mandla announced the ACS software quality accreditation policy in an address to the Software Industry Action Group conference, being hosted by Software Engineering Australia (SEA) in Melbourne.

### 4C5 Academic/Industry/Vendor/Govt efforts

2004-02-25	computer security firms alliance secure US communication networks
Category 4C5	Academic/Industry/Vendor/Govt efforts

NewsScan

COMPUTER SECURITY FIRMS FORM NEW ALLIANCE

Eleven top U.S. computer security firms have banded together to form the Cyber Security Industry Alliance, a lobbying group that hopes to work cooperatively with Congress to come up with a plan for securing the nation's electronic communications networks. "Rather than saying to Congress, "This is not an issue, stay out,' we as an industry need to figure out how to solve thee problems in a proactive way before someone gets fed up and says it's time to legislate," says Sanjay Kumar, CEO of Computer Associates. One of the Alliance's first tasks will be to develop common standards for reporting and sharing information on Internet security threats. Former White House technology adviser Richard Clarke says the proliferation of malicious worms and viruses in 2003 has fueled demand for action: "Last year was the worst in history in terms of the damage from cyber-attacks. I think we're getting to the point where Congress wants something to happen, the people and American corporations that buy information technology want something to happen, and so having the technology security industry organized to be part of that debate makes a lot of sense." Other companies involved in the Alliance include: Bindview Corp., Check Point Software Technologies (a subsidiary of Juniper Networks), PGP Corp., RSA Security and Secure Computing Corp. (Washington Post 25 Feb 2004)

Category	4C5	Academic/Industry/Vendor/Govt efforts
Category	4C5	Academic/Industry/Vendor/Govt efforts

#### 2004-03-18 cybersecurity network US National Partnership

NewsScan

PROPOSED CYBERSECURITY NETWORK

The National Cyber Security Partnership (which includes the U.S. Chamber of Commerce, the Business Software Alliance and the TechNet lobbying group) is asking Congress for money to create a cybersecurity information clearinghouse for the business community. The group's recommendations include development of a "Home User Cyber Security Tool Kit" and the designation of a "cyber security month." The clearinghouse would be known as the "National Crisis Coordination Center." (Washington Post 18 Mar 2004)

Category 4C5 Academic/Industry/Vendor/Govt efforts

2004-04-01 softeware industry acknowledges network security Bush administration

DHS IAIP Daily;

http://www.cnn.com/2004/TECH/internet/04/01/cybersecurity.ap /index.html

April 01, Associated Press — Software industry makes room for government.

In a surprise shift, leading software companies acknowledge in a report to the Bush administration that the government might need to force the U.S. technology industry to improve the security of America's computer networks. The companies, including Microsoft Corp. and Computer Associates International Inc., said the Homeland Security Department "should examine whether tailored government action is necessary" to compel improvements in the design of computer software. The 250- page report containing that recommendation and dozens more was being released Thursday, April 1. It cautioned that government should require security improvements only when market forces fail. It also said businesses already are demanding software that is safer and more resilient to attacks. But the report said the most sensitive computer networks - - such as those operating banks, telephone networks or water pipelines - - "may require a greater level of security than the market will provide." In those cases, the software companies recommend "appropriate and tailored government action that interferes with market innovation on security as little as possible." It urged the government to work with companies to produce a formal study during the 2005 fiscal year, which begins in October.

Category 4C5 Academic/Industry/Vendor/Govt efforts

2004-04-01 computer crime vandalism government role reduction

NewsScan

FIGHTING COMPUTER MISCHIEF

An industry task force is advising the federal government to set goals for reducing hacking, spam, worms, viruses and identity fraud -- though the group has refrained from offering specific measures. Indicating the need for the federal government to play a stronger role in computer security issues, the report calls for increased funding for cyber-security research at universities; improved university certification programs that stress security training for engineers; and a Department of Homeland Security evaluation of software vulnerabilities. Alan Paller of the SANS Institute, a computer-security research group, is critical of the report: "What we got was not solutions, but a description of the problem," in which "there's nothing about the companies that make billions of dollars selling this broken stuff." Task Force co-chairman Ron Moritz of Computer Associates insists: "We're far from doneMoritz says executives will have to go back and tell their programmers: "You've been doing this wrong for the past 25 years." (Washington Post 1 Apr 2004)

Category 4C5 Academic/Industry/Vendor/Govt efforts

2004-04-06 industry security improvements cybersecurity recommendations corporate practice

DHS IAIP Daily;

http://www.fcw.com/fcw/articles/2004/0405/web- putnam- 04- 06- 0 4.asp

April 06, Federal Computer Week — Industry suggests security improvements.

The Corporate Information Security Working Group, which Rep. Adam Putnam (R- FL) convened five months ago, issued several lists of cybersecurity recommendations that Putnam has promised to review before considering any new security legislation on Tuesday, April 6. Most of the recommendations from the group's call on the federal government to provide incentives for good corporate security practices, but they reject any substantial role for the federal government in policing the information security practices of corporations. The group made recommendations on best practices, education, incentives, information sharing and procurement practices. One recommendation was to amend the Clinger- Cohen Act of 1996 to require that federal agencies include computer information security in making IT strategic plans and spending decisions. The recommendations are available online:

http://reform.house.gov/TIPRC/News/DocumentSingle.aspx?Docum entID=3030

Category 4C5 Academic/Industry/Vendor/Govt efforts

2004-05-18 data sharing security bridge federal government PKI federated identity

DHS IAIP Daily;

http://www.fcw.com/fcw/articles/2004/0517/web- pki- 05- 18- 04.a sp

May 18, Federal Computer Week — Three agencies, supplier certified for security bridge.

Three federal agencies and a federal supplier have achieved cross- certification status with the Federal Bridge Certification Authority, a secure systems infrastructure for exchanging data. The admission of four new members doubles the number of organizations that have passed rigorous tests required for cross- certification with the bridge, federal officials announced at a recent Federal Public Key Infrastructure (PKI) Deployment Workshop in Washington, DC. Cross- certification means the eight federal agencies and supplier with that status can exchange sensitive information online knowing that the other cross- certified agencies' digital signatures and certificates be trusted. The conceptual architecture that includes the bridge has been expanded to include newer security policy concepts such as those defined by the Office of Management and Budget's E- Authentication program. But officials said the federal bridge continues to play an important role in secure data exchanges among agencies and among the federal government and the states, other countries and businesses. Category 4C5 Academic/Industry/Vendor/Govt efforts

2004-05-18data sharing government portal

DHS IAIP Daily;

http://fcw.com/fcw/articles/2004/0517/web- irish- 05- 18- 04.asp

May 18, Federal Computer Week — When Irish eyes are sharing.

Using a central portal for citizen services, Irish officials are allowing agencies to share information while ensuring that agencies retain their autonomy. "The idea is agencies don't talk directly to each other," said Sean McGrath, chief technology officer of business integration company Propylon, 11 speaking Monday, May 17 on a panel at the CIO Summit. "They talk to a single hub." That hub is at the heart of the Public Services Broker, which provides citizens with a single point of access to government services and allows for data sharing governmentwide. Rather than share information directly, agencies provide data to a central location, which packages and disseminates the requested information. This approach is faster and cheaper than distributed architectures and allows for flexibility and ownership among agencies. The Public Services Broker portal will go live next month, said Oliver Ryan, director of Ireland's Reach agency.

Category 4C5 Academic/Industry/Vendor/Govt efforts

2004-05-20 Federal Enterprise Architecture FEA government OMB security layer

DHS IAIP Daily; http://www.gcn.com/vol1\_no1/daily- updates/25994- 1.html

May 20, Government Computer News — FEA security layer due this summer.

The Office of Management and Budget (OMB) by the end of the summer will release a security layer for the Federal Enterprise Architecture (FEA). Environmental Protection Agency CIO Kim Nelson, the co- chairwoman of the CIO Council's Architecture and Infrastructure Committee, told lawmakers yesterday that committee members are reviewing CIO comments on the plan and will release it soon to be used by agencies. OMB decided to make security a layer that cuts across all the FEA reference models, instead of separate reference model, because of its importance to every aspect of the IT planning, design and implementation processes, said Karen Evans, OMB administrator for e- government and IT.

Category 4C5 Academic/Industry/Vendor/Govt efforts

outsource government network services treasury

DHS IAIP Daily;

2004-05-24

http://fcw.com/fcw/articles/2004/0524/tec- treasury- 05- 24- 04. Asp

May 24, Federal Computer Week — Treasury to outsource network services.

By the end of the year, U.S. Department of Treasury officials expect to award what could be the federal government's largest telecommunications contract for managed services. The new contract will be based on service- level agreements, which private- sector officials increasingly view as the most efficient way of buying telecom services. "We want obviously the best service for the cheapest price, as any organization would," said Mike Parker, acting chief information officer at Treasury. Department officials said they expect to use the managed services contract to acquire such advanced network capabilities as IP multicast, IP Version 6, IP telephony and optical- wavelength service. IP multicast is a way to broadcast video signals via networks that use relatively low bandwidth. The contract will cost Treasury as much as \$1.5 billion, but it will get the agency out of the telecom business. It will no longer own the network assets on which it will depend.

Category 4C5 Academic/Industry/Vendor/Govt efforts

2004-06-01 Internet access satellite television broadcast

NewsScan

NEWS CORP. SCRAPS SATELLITE INTERNET PLANS

News Corp. is dropping plans to deliver broadband Internet access via satellite in the U.S. The company says it will still launch at least one Spaceway satellite, but will use it for television broadcast, not high-speed Internet service. The announcement came as a surprise to News Corp. subsidiary DirecTV, which disputed its parent company's statement, saying "we have not scrapped plans to use the satellites for broadband access. In fact, the satellites are being designed specifically so they can be used for video or broadband." (Reuters/CNet 1 Jun 2004)

Category 4C5	Academic/Industry/Vendor/Govt efforts
2004-06-07	Microsoft Windows XP software strategy developing countries
MarriaCoon	

NewsScan

SPECIAL SOFTWARE STRATEGIES FOR DEVELOPING COUNTRIES

Departing from a one-size-fits-all global pricing strategy, Microsoft has tailored special government-promoted PC sales for Thailand and Malaysia in a new marketing approach for emerging markets. Localized versions of Microsoft Windows XP are offered without English-language support, and the company is apparently developing leaner Windows with features more appropriate to developing countries. Microsoft executive Barry Goff says, "This is a new market with very different needs, from an economic perspective, from a social perspective, from a technical perspective." In addition Microsoft, companies such as Symantec and Sun Microsystems have also introduced special government pricing strategies for developing countries. Jupiter Research industry analyst Joe Wilcox says, "What we're seeing is the beginning of a trend. The more companies test the waters, the more of a trend there is because of the competitive threat." (AP/San Jose Mercury News 7 Jun 2004)

Category 4C5 Academic/Industry/Vendor/Govt efforts

#### 2004-06-24 Brazil lawsuit Microsoft attacked Australia OSIA Bill Gates

NewsScan

MICROSOFT'S BRAZIL LAWSUIT 'REPREHENSIBLE'

OSIA, Australia's Open Source industry body, has issued a scathing criticism of Microsoft's lawsuit against Sergio Amadeu, President of the Brazilian National Institute for Information Technology, calling it a "reprehensible action" that attempts to "curb freedom of speech and of

criticism." The defamation lawsuit was filed after Amadeu defended the Brazilian government's decision to shift 300,000 PCs from Windows to Linux. He had said this decision "makes sense for a developing country where a mere 10% of the 170 million people have computers at home and where the debt-laden government is the nation's biggest computer buyer." OSIA also referred to Microsoft's "abuse" of its monopoly position, and Bill Gates's address to university students in 1998, where he made a statement saying, "Although about 3 million computers get sold every year in China, people don't pay for the software. Someday they will, though. As long as they are going to steal it, we want them to steal ours. They'll get sort of addicted, and then we'll somehow figure out how to collect sometime in the next decade." (The Age, 24 Jun 2004)

Category 4C5 Academic/Industry/Vendor/Govt effo	orts
---	------

2004-07-19 Microsoft software anti-trust Justice Department compliance question

NewsScan

IS THE NEW MICROSOFT SOFTWARE ANTITRUST-COMPLIANT?

The Justice Department has told a federal judge that the government wants to look at Microsoft's next-generation operating system (code-named Longhorn) early enough that changes can still be made in it if they are necessary for compliance with the antitrust agreement made two years ago.

Industry analysts have predicted introduction of Longhorn in 2006 or 2007, when the antitrust settlement is scheduled to expire. A Microsoft spokesman says, "All development is being done with full consideration for our obligations and commitments," and U.S. District Judge Colleen Kollar-Kotelly, who presided over the antitrust agreement, praises its effectiveness so far. (Washington Post 19 Jul 2004)

### Category4C5Academic/Industry/Vendor/Govt efforts2004-07-30Georgia Fulton County network security upgrade bandwidth usage

DHS IAIP Daily;

http://www.informationweek.securitypipeline.com/news/2610099 8

July 30, InformationWeek — Georgia County looks at network traffic.

The Department of Information Technology in Fulton County, GA, has just completed a network- security upgrade that gives it the ability to detect the amount of network resources being consumed by applications across the county's 5,500 PCs. Use of instant messaging, radio broadcasts over the Web, and peer- to- peer file sharing apps such as Kazaa are not new to the county. But their proliferation had recently begun "eating up bandwidth that I'm purchasing with taxpayer dollars," says county CIO and IT director Robert Taylor. Not a good thing, particularly as Fulton County expands its E- government initiatives to provide its 886,000 residents with greater access to county records via the Web. Rather than buying additional DS3 lines, which run at around 45 Mbps and cost about \$8,000 per month, Taylor and his staff decided to make better use of the network's existing bandwidth. The upgrade will also improve security. The network was hit last October by a denial- of- service attack caused by the Welchia virus, an aggressive infection designed to exploit a software flaw in recent versions of Windows. Although the virus was contained, Smith says, the server is being used to identify malicious behavior before it becomes a problem.

Category 4C5 Academic/Industry/Vendor/Govt efforts

2004-08-04 Federal Communications Commission FCC network outage reporting rules

DHS IAIP Daily;

http://hraunfoss.fcc.gov/edocs\_public/attachmatch/DOC- 250543 A1.pdf

August 04, FCC — FCC adopts rules to enhance network outage reporting.

The Federal Communications Commission (FCC) on Wednesday, August 4, adopted new rules requiring wireless, wireline, cable, and satellite telecommunications providers to report information electronically to the FCC about significant disruptions or outages to their communications systems. The Commission also ruled that all sensitive information collected as a result of these new rules will be protected from public disclosure. These actions will facilitate more reliable telecommunications throughout the United States and promote homeland security, building on the telecommunications industry's efforts to date to improve outage reporting. Under the new rules, both wireless and satellite providers will be subject to the FCC's reporting requirements. The increasing use of cell phones and pagers, as well as the Nation's growing dependence on satellite communications as critical infrastructure, necessitated these changes to the Commission's rules. Action by Report and Order and Further Notice of Proposed Rulemaking (FCC 04- 188).

Category 4C5 Academic/Industry/Vendor/Govt efforts

2004-08-27 cybersecurity memo required Office of Management and Budget OMB

DHS IAIP Daily; http://www.gcn.com/vol1\_no1/daily- updates/27089- 1.html

August 27, Government Computer News — OMB asks agencies for cybersecurity check- up.

Agencies have until October 6, 2004 to report to the Office of Management and Budget (OMB) on how they have improved their cybersecurity over the past year. In a memo to agency executives, OMB director Joshua B. Bolten said agencies should summarize the results of their annual IT security reviews of systems, agency progress in correcting weaknesses defined in their plans of actions and their inspector general evaluations. Last year, agencies said about 62 percent of all systems were secured, and OMB earlier this month, said that number had increased to 70 percent. Agencies still are well behind the administration's goal of 90 percent of all systems secured by December 2003.

Category 4C5 Academic/Industry/Vendor/Govt efforts

2004-09-21 America Online AOL second level security subscription

NewsScan

AOL OFFERS SECOND LEVEL OF SECURITY

AOL has become the first major U.S. online business to offer customers a second layer of security, which it will make available to subscribers for \$1.95 a month in addition to a one-time \$9.95 fee. The system uses a matchbook-size device displaying a six-digit log-on code that changes every minute; it requires that the second password be entered in order to check e-mail or access such services as calendars, stock portfolios and AOL's Bill Pay. Gartner analyst Avivah Litan estimates that no more than 5-15% of AOL subscribers will sign up initially but says that "you have to start somewhere." (AP/Washington Post 21 Sep 2004)

# Category 4C5 Academic/Industry/Vendor/Govt efforts 2004-10-11 National Institute of Standards and Technology NIST minimum security concerns document publication

DHS IAIP Daily;

http://www.fcw.com/fcw/articles/2004/1011/web- nist- 10- 11- 04. asp

October 11, Federal Computer Week — NIST details minimum security controls for federal information systems.

A new document by the National Institute of Standards and Technology (NIST) spells out the minimum security controls that federal agency officials must use to comply with the statutory requirements of the Federal Information Security Management Act of 2002. The document, Special Publication 800- 53, will be available at www.nist.org until November 30 for public review and comment. NIST officials said they are especially interested in receiving comments about the cost and potential impact that the recommended computer security controls could have on federal agencies.

#### Category 4C5 Academic/Industry/Vendor/Govt efforts

#### 2004-10-18 security Microsoft Cisco alliances Dell AOL Yahoo spyware customers

NewsScan; http://www.washingtonpost.com/wp-dyn/articles/A41629-2004Oct18.html

#### SECURITY PROBLEMS PROMPT STRANGE BEDFELLOWS

With security looming as major issue for users, top technology firms are coming to terms with the need to form alliances in order to combat the plague of viruses, computer worms and spyware programs that threatens computing productivity. One case in point is today's announcement that Microsoft and Cisco are teaming up to tackle the problem, in an acknowledgement that many corporate customers have made major investments in both companies' technology and do not want to be forced to choose between them when it comes to security solutions. Meanwhile, Dell is partnering with the nonprofit Internet Education Foundation -- a coalition that includes tech giants like AOL and Yahoo -- to educate consumers about the risks of spyware. Dell VP Mike George says his company normally does not become involved in software issues, but in recent months has stepped up efforts to help consumers rid their computers of spyware and other problems because they are turning off potential users.

Category 4C5 Academic/Industry/Vendor/Govt efforts

#### 2004-11-04 Microsoft patch issue help preparation security bulletin publication Website

DHS IAIP Daily;

http://www.infoworld.com/article/04/11/04/HNmicrosoftpatchin g\_1.html

November 04, IDG News Service — Microsoft to help users prepare for patching.

Microsoft Corporporation will give customers advance notice of its monthly security updates in an effort to help them prepare to install related software patches, the company announced Thursday, November 4. Starting this month, Microsoft will publish on its Website a summary of planned security bulletins three days before they are released in their entirety. The summary will include information on which products are affected by updates, and severity ratings for security problems. The company normally releases security bulletins on the second Tuesday of each month. It previously offered customers who signed up through support personnel advanced notifications, but the information was not published for all customers. The information will be available at http://www.microsoft.com/technet/security/default.mspx

Category 4C.	5 Academic/1	Industry/Vendor/	Govt efforts
--------------	--------------	------------------	--------------

### 2004-11-17 Carnegie Mellon University CMU Korean Information Security Agency collaboration CyLab

DHS IAIP Daily; http://www.cmu.edu/cmnews/extra/041116\_cylab.html

November 17, Carnegie Mellon University — Carnegie Mellon to create collaborative research lab with Korea Information Security Agency.

Carnegie Mellon University and Korean officials have agreed to create a new collaborative research lab for the study and development of leading- edge security technologies. Officials from the Korea Information Security Agency (KISA) have pledged \$6 million over the next three years to establish CyLab Korea at Carnegie Mellon. KISA will also establish CyLab Korea in Seoul, Korea, with more than 10 research staff members. Both sites will work together on research projects and develop new technologies and paradigms that will usher in an era of more secure computers, networks and communications systems. KISA is a center of excellence responsible for the computer network security of commercial information technology infrastructure that covers nearly 90 percent of the entire infrastructure of information technology in the Republic of Korea (South Korea).

Category 4C5 Academic/Industry/Vendor/Govt efforts

#### 2004-11-18 Oracle patch cycle security planning no surprise

DHS IAIP Daily; http://www.informationweek.com/showArticle.jhtml;jsessionid= CNBEG43XHVO1YQSNDBGCKH0CJUMEKJVN?articleID=53700526

November 18, InformationWeek — Oracle moves to quarterly security- patch cycle.

Oracle's new quarterly patch schedule comes only months after the company said it would issue such security updates every month. The company says patches will be published simultaneously to all customers through its Web support site MetaLink each quarter beginning on January 18. Oracle says the new schedule will allow its customers to plan to patch, rather than react to "surprise" patch alerts.

2004-11-27	UK IT computer network sprawl chaos failure prevention project healthcare banking
Category 4C5	Academic/Industry/Vendor/Govt efforts

DHS IAIP Daily; http://www.newscientist.com/news/news.jsp?id=ns99996706

November 27, New Scientist — Sprawling systems teeter on IT chaos.

The UK government is spearheading a \$19 million program aimed at finding ways to avert catastrophic failures in large IT networks. Some systems are now so large they are untestable, making it impossible to predict how they will behave under all circumstances. The hidden flaws could lead to crashes in critical networks like healthcare or banking systems. The scheme has been given added urgency by the failures of power grids in the U.S. and Italy last year. There is a real danger that such massive interconnected systems will exhibit potentially disastrous "emergent behaviors," says David Cliff of Hewlett- Packard's laboratory in Bristol, UK. The \$19 million the UK is to spend will be used to set up a national center to study IT complexity, managed by the Engineering and Physical Sciences Research Council.

Category 4C5	Academic/Industry/Vendor/Govt efforts
2004-11-30	University Texas cybersecurity research center CIAS technology multi disciplinary
	initiative

DHS IAIP Daily; http://austin.bizjournals.com/austin/stories/2004/11/29/dail y13.html?jst=b\_ln\_hl

November 30, Austin Business Journal (TX) — UT's info security center to address cybersecurity concerns.

The University of Texas has established a new security center to address the growing cybersecurity problems across the country. The Center for Information Assurance and Security's (CIAS) goal is to conduct research that will lead to innovative cybersecurity solutions and address the national need to produce more trained professionals in the field. "Despite considerable industry spending to develop solutions, the cybersecurity problem continues to grow at an alarming rate," says Frederick Chang, director of the CIAS and a research professor. The new center will involve business, government and academia in its effort to be a multi- disciplinary initiative.

Category 4C5 Academic/Industry/Vendor/Govt efforts

2004-12-02 United States US Japan cooperation cybersecurity information networks security global culture

DHS IAIP Daily; http://tokyo.usembassy.gov/e/p/tp- 20041202- 05.html

December 02, U.S. Department of State — United States, Japan should cooperate on cybersecurity.

The United States and Japan should intensify cooperative efforts to secure their information networks and work toward the creation of "a global culture of cyber security," according to Lincoln P. Bloomfield Jr., assistant secretary of state for political- military affairs. Bloomfield addressed the U.S.- Japan Critical Information Systems (CIP) Forum hosted by the Vanderbilt Institute for Public Policy Studies in Washington, DC on Tuesday, November 30. "Weaponizing" information technology (IT) is relatively cheap and attacks can be carried out with "a reasonable expectation of impunity," according to Bloomfield. For this reason, the United States and Japan must join forces to protect their own and global information systems, he said. The two countries' governments have made steps in this direction, Bloomfield pointed out. The first formal discussion of cybersecurity began in June 2002, and efforts continued with meetings in February 2004. Each nation must take systematic, coordinated actions to protect its own networked information systems, Bloomfield said. Global efforts to secure information systems, he said, include not just governments but information technology developers, vendors, data managers, and telecom providers.

# Category 4C5 Academic/Industry/Vendor/Govt efforts 2004-12-14 General Services Administration GSA security working group revival standards evaluation

DHS IAIP Daily; http://www.gcn.com/vol1\_no1/daily- updates/30948- 1.html

December 14, Government Computer News — GSA will revive security working group.

The General Services Administration (GSA) will re- establish a government- wide working group to evaluate telecommunications security and draft standards. The effort will be part of GSA's Multitier Security Profile Program, an effort to package security services for agencies, said John Johnson, assistant commissioner for service development at GSA's Federal Technology Service. He said the working group would be in place within two months. Because of the importance of security, the new group will remain in place indefinitely, Johnson said. It will build on the early work to look at changes in telecomm security needs and recommend standards, he said.

### 4D Funny / miscellaneous

Category 4D	Funny / miscellaneous		
2004-01-06	puns computer Internet security funny		
RISKS		23	14
PUN-INTENDED I	DEFINITIONS		
RISKS moderator Peter Neumann lists a few pun-ful computer-related definitions from _The Sunday San Jose Mercury_ (January 4, 2004):			
off-shorn: vt. Gettin	g cut because your job moved overseas. [Rainer Richter, San Jose]		
Microsofa: n. A piece of furniture that, while it looked fine in the showroom, gradually begins to dominate the living room, eventually forcing you to replace all the other furniture, including the TV, to be "compatible". [Earl T. Cohen, Fremont]			
motherbored: n. In many homes, a technology discussion at dinner between father and the kids. (Bruce Kerr)			
Luddate: n. Someone you are going out with who does not understand the [Santa Clara] Valley's obsession with technology. (Lisa Lawrence, Palo Alto)			
Crisco: n. A person	who got fried by buying Cisco at \$80 a share. (Jim Schutz)		

Category 4DFunny / miscellaneous2004-01-12Potato computer scam Germany fraud

NewsBits; http://zdnet.com.com/2110-1105\_2-5139288.html

'Potato' computer scam under investigation

German police are investigating after an angry man returned a computer he had just bought saying it was packed with small potatoes instead of computer parts. The store replaced the computer free of charge but became suspicious when he returned a short time later with another potato-filled computer casing, police in the western city of Kaiserslautern said on Monday. ``The second time he said he didn't need a computer any more and asked for his money back in cash," a police spokesman said. Police are now investigating the man for fraud.

Category 4D Funny / miscellaneous

#### psychology cyberspace honesty open up online permanent records

2004-03-21 NewsScan

THE ONLINE HONESTY PARADOX

Cornell University professor Jeffrey Hancock conducted an experiment recently that concluded people are less likely to fib online than when talking in person or on the phone. While this proposition flies in the face of warnings over psycho-weirdos lurking in chat rooms and on cyber-dating sites, New York Times columnist Clive Thompson says actually it makes sense, considering the relative durability of the e-mail message. While a lie spoken in person or over the phone can later be denied, on the Internet, your words may come back to haunt you. "Today's titans of industry are laid low not by ruthless competitors but by prosecutors gleefully waving transcripts of old e-mail, filled with suggestions of subterfuge... We all read the headlines; we know that in cyberspace our words don't die, because machines don't forget." A second contributing factor, says Thompson, is that there's "something about the Internet that encourages us to spill our guts, often in rather outrageous ways. Psychologists have noticed for years that going online seems to have catalytic effect on people's personalities." Indeed, an experiment conducted by Open University psychologist Adam Johnson found that strangers chatting online were much more likely to offer up personal details about themselves than when conversing face-to-face. "Our impulse to confess via cyberspace inverts much of what we think about honesty," says Thompson, citing the current corporate convention of flying cross-country for that allimportant five-minute face-to-face meeting before signing off on a deal. Instead, Thompson suggests that "as more and more of our daily life moves online, we could find ourselves living in an increasingly honest world, or at least one in which lies have ever more serious consequences." (New York Times 21 Mar 2004)

#### Category 4D Funny / miscellaneous

#### super computer laptop flash mob gathering processing power

#### DHS/IAIP Update

2004-03-30

March 29, New Scientist — Flash mob to attempt supercomputing feat.

An attempt to transform a motley collection of laptops into the first ad- hoc supercomputer is scheduled for April 3 at the University of San Francisco. Over 1000 laptop owners will gather in the university gym in an attempt to build a "flash mob" supercomputer. The project's organizers hope that FlashMob will run fast enough to beat supercomputers in the list of the world's top 500 supercomputers. One of the challenges facing John Witchel, the USF graduate student running the project, and his colleagues, is that "You essentially don't know anything about the computers until they show they up that day." The team therefore had to write code that not only allows the computers to share lots of data quickly, but also determines each processor's speed and memory as it goes. This allows the computational tasks to be allocated in the most efficient way possible. To beat the slowest computer in the top 500, FlashMob will have to perform a rigorous mathematical calculation called Linpack at a rate of at least 403 billion flops (floating point operations per second).

Category 4D Funny / miscellaneous

#### 2004-05-04 computers health research disease fighting MIDAS initiative NIH

DHS IAIP Daily; http://www.nih.gov/news/pr/may2004/nigms- 04.htm

May 04, National Institutes of Health — Computers combat disease.

A new initiative, called MIDAS, will develop powerful computer modeling techniques to analyze and respond to infectious disease outbreaks, whether they occur naturally or are released intentionally in a bioterrorist attack. MIDAS is sponsored by the National Institute of General Medical Sciences (NIGMS), a part of the National Institutes of Health (NIH). NIGMS recently awarded the first four grants in this new initiative, totaling more than \$28 million over five years. Three of these grants will support the creation of mathematical models to study various aspects of infectious disease epidemics and community responses. These research grants together total \$9.5 million over five years. A fourth award, totaling \$18.8 million over five years, funds researchers to develop a central database to organize information from the other three groups. It also supports the development of user- friendly computer modeling tools for the broader scientific community, policy makers and public health officials to use to simulate epidemics, and response strategies.

Category 4D Funny / miscellaneous

#### 2004-05-17 cartoon character terrorist intelligence search engine homeland security

NewsBits;

http://www.usnews.com/usnews/issue/040517/whispers/17whisplead\_2.htm

THE GOOGLE TERRORIST

It was the lead item on the government's daily threat matrix one day last April. Don Emilio Fulci described by an FBI tipster as a reclusive but evil millionaire, had formed a terrorist group that was planning chemical attacks against London and Washington, D.C. That day even FBI director Robert Mueller was briefed on the Fulci matter. But as the day went on without incident, a White House staffer had a brainstorm: He Googled Fulci. His findings: Fulci is the crime boss in the popular video game Headhunter. "Stand down," came the order from embarrassed national security types.

Category 4D Funny / miscellaneous

2004-06-01 online newspaper reading increase India China Russia news entertainment

NewsScan

ONLINE NEWSPAPER READERSHIP UP 350% OVER 5 YEARS

The audience for online versions of newspapers has grown 350% over the past five years, according to the World Association of Newspapers, which notes that while print circulation figures have declined in mature markets like Europe and the U.S., they are sharply up in emerging markets

like China and India. In Russia, the number of published dailies has nearly doubled in two years. WAN attributed the increase in online newspaper popularity to the growth of broadband in many countries, noting that in those countries where broadband Internet access is more readily available,

people are watching TV less and surfing the Web more, both for news and for entertainment. (BBC News 1 Jun 2004)

## Category 4DFunny / miscellaneous2004-06-14Matsuhita Eletric Japan sleep room 30-minute assessment sleep deprived profile

NewsScan

#### MATSUSHITA DEBUTS HIGH-TECH 'SLEEP ROOM'

Matsushita Electric Works is taking the wraps off its "Sleep Room" next week in Tokyo, giving the sleep-deprived a chance to analyze their sleep patterns and catch 40 winks while they're at it. The company says its new product is geared toward the growing market of insomniacs in a country

where students start burning the midnight oil in elementary school -- a pattern that's then replicated in the typical workday. A Health Ministry survey indicated in 2000 that 31% of Japanese don't get enough sleep because of work, school or long commuting times. Another 29% cited stress

as a prime source of wakefulness. At Matsushita's "Vitality Diagnostic Corner," visitors are greeted by a "sleep counselor" who leads them through a 30-minute software program designed to pinpoint sleep problems and develop a "sleep profile." Customers can then try out a 30-minute session

in the sleep room, where they're greeted by a wall-sized TV displaying a soothing river scene surrounded by forest and augmented by gentle guitar and piano music blended with gurgling water and bird sounds. After a few minutes, the lights dim, the TV screen goes blank, and the bed's mattress kicks into gear, vibrating and kneading strategically to administer a massage and ease the customer into sleep. After 30 minutes, the lights slowly come on and the TV displays a crystal lake, while the bed gradually cranks up to a sitting position. The company plans to market the device to

homeowners for \$30,000, and says even though the price is high, there will be takers. "Nobody who's come in here for 30 minutes hasn't fallen asleep," says a Matsushita official. (AP/USA Today 14 Jun 2004)

Category 4D Funny / miscellaneous

#### 2004-08-15 supercomputer link security 150 fastest US Department of Energy

DHS IAIP Daily;

http://www.eweek.com/article2/0%2C1759%2C1636023%2C00.asp

August 15, Associated Press — Computer could link workers, stay secure.

A new supercomputer could join workers at the Idaho National Engineering and Environmental Laboratory in Idaho Falls, ID, with colleagues in France, Chile and across the U.S. while keeping sensitive information secure. The system could reach speeds of up to 1,500 gigaflops, making it one of the 150 fastest supercomputers in the world, officials said. Calculations and models that formerly took researchers a year will only take days to complete using the new system, officials said. Researchers will use the supercomputer to design the next generation of nuclear power plants, research the cause of mad cow disease and develop microbes that can eat heavy metals to use cleaning up contaminated sites. Those outside the laboratory must be approved by the U.S. Department of Energy to use the system. The computer can isolate information, essentially giving each user its own part of the system to control, Greenwade said.

Category 4D Funny / miscellaneous

#### 2004-08-26 Friday no e-mail Veritas employee communication face-to-face

NewsScan

COULD 'E-MAIL-FREE' FRIDAYS REPLACE KHAKIS AND KNIT SHIRTS?

We all know that e-mail is turning into a huge time and productivity sink, but one lone crusader in Silicon Valley is trying to do something about it. Two months ago Jeremy Burton at Veritas Software decreed that Fridays in his marketing department were to be "e-mail free" -- employees

who needed to communicate with each other were instructed to stop by and chat or use the phone. "E-mail is supposed to be this big productivity tool, but it's getting to the point where it is out of control," says Burton, who complains that he was regularly spending two hours a day just dealing with e-mail. The ban applies only to interdepartmental communications and violators are fined \$1 per transgression, with the proceeds going toward charity (so far, almost \$70 has been collected). Many workers have endorsed the ban, noting the advantages of face-to-face conversations, and Burton says he plans to continue the policy indefinitely. (Wall Street Journal 26 Aug 2004)

# Category 4D Funny / miscellaneous 2004-11-02 study top technology nations world Information Society Index ISI Denmark Sweden US Switzerland

DHS IAIP Daily;

http://management.silicon.com/careers/0,39024671,39125505,00.htm

November 02, Silicon.com — Top tech nations revealed.

Denmark is the most technologically savvy nation, taking the top spot from Sweden. Sweden is now second, followed by the U.S., Switzerland and Canada. The rankings are based on the IDC Research's Information Society Index (ISI), which aims to measure the ability of 53 countries to access and use information technology. IDC rates each country on a total of 15 variables in four areas: computers, internet, telecoms and social. David Emberley, senior analyst for the IDC, noted a new trend this year - less of a link between social and technology scores. Previously companies with high social rankings tended to have a high level of technology. Report: http://www.idc.com/groups/isi/main.html